AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

Public Power
CYBER INCIDENT RESPONSE PLAYBOOK

August 2019

Acknowledgment: This material is based upon work supported by the Department of Energy under Award Number(s) DE-OE0000811.

Playbook Development

NEXIGHT GROUP

This Playbook was developed by Nexight Group with technical support from the American Public Power Association and its members. We would like to acknowledge the following individuals who provided their time, resources, and knowledge to the development of this Playbook:

Public Power Utilities

Bernie Acre, *Bryan Texas Utilities*
Cheryl Anderson, *Florida Municipal Electric Association*
Bill Berry, *Owensboro Municipal Utilities*
Randy Black, *Norwich Public Utilities*
David Boarman, *Owensboro Municipal Utilities*
Phil Clark, *Grand River Dam Authority*
Jim Compton, *Burbank Water and Power*
Josh Cox, *City of Westerville*
Adrian de la Cruz, *Kerrville Public Utility Board*
Maggie Deely, *American Municipal Power, Inc.*
Colin Hansen, *Kansas Municipal Utilities*
Jennifer Keesey, *Northwest Public Power Association*
Branndon Kelley, *American Municipal Power, Inc.*
Mike Klaus, *Central Nebraska Public Power & Irrigation Dist.*
Kurt Knettel, *New Braunfels Utilities*
Matt Knight, *Owensboro Municipal Utilities*
Melvyn Kwek, *Guam Power Authority*
Matt Lee, *Platte River Power Authority*
Ken Lewis, *Salt River Power*
Chris Lindell, *Beatrice City Board of Public Works*
Carter Manucy, *Florida Municipal Power Agency*
Robby McCutcheon, *Kerrville Public Utility Board*
Rob Morse, *Platte River Power Authority*
Michelle Nall, *Glendale Water & Power*
Erik Norland, *Chelan Public Utility District*
Steve Schmitz, *Omaha Public Power District*
Chad Schow, *Franklin Public Utility District*
Kenneth Simmons, *Gainesville Regional Utilities*
Scott Smith, *Bryan Texas Utilities*
Howard Wong, *Glendale Water & Power*

Association Staff

Jack Cashin, *American Public Power Association*
Chris Ching, *American Public Power Association*
Meena Dayak, *American Public Power Association*
Alex Hofmann, *American Public Power Association*
Nathan Mitchell, *American Public Power Association*
Sam Rozenberg, *American Public Power Association*
Giacomo Wray, *American Public Power Association*

Association Partners

Kaitlin Brennan, *Edison Electric Institute*
Jason Christopher, *Axio Global*
Chris Kelley, *Beam Reach Consulting Group*
Lindsay Kishter, *Nexight Group*
Aaron Miller, *MS-ISAC*
John Meckley, *Edison Electric Institute*
Mark Mraz, *Beam Reach Consulting Group*
Jason Pearlman, *Nexight Group*
Valecia Stocchetti, *MS-ISAC*
Paul Tiao, *Hunton Andrews Kurth*

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government to protect the interests of the more than 49 million people that public power utilities serve, and the 93,000 people they employ. Our association advocates and advises on electricity policy, technology, trends, training, and operations. Our members strengthen their communities by providing superior service, engaging citizens, and instilling pride in community-owned power.

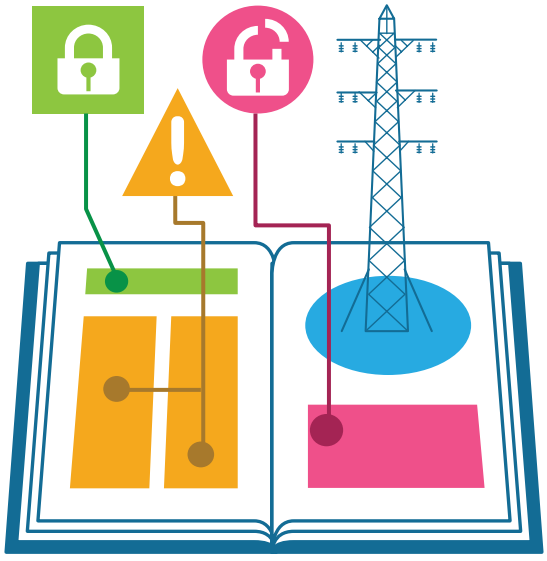
Table of Contents

1 EXECUTIVE SUMMARY

How to Use the Playbook

The Playbook provides step-by-step guidance for small to mid-sized public power utilities to help them prepare a cyber incident response plan, prioritize their actions and engage the right people during cyber incident response, and coordinate messaging. The playbook serves three key purposes:

1. Provides guidance to help a utility develop its cyber incident response plan and outline the processes and procedures for detecting, investigating, eradicating, and recovering from a cyber incident.
2. Maps out the industry and government partners that public power utilities can engage during a significant cyber incident to share information, get support for incident analysis and mitigation, and coordinate messaging for incidents that require communication with customers and the public.
3. Outlines the process for requesting cyber mutual aid from utilities across the energy industry for a cyber event that significantly disrupts utility business or operational energy delivery systems and overwhelms in-house cyber resources and expertise.



Overview of Playbook Guidance

This Playbook provides utilities with practical guidance and critical considerations in preparing for a cyber incident and developing a response plan that enables staff to take swift, effective action. Cybersecurity managers can use the playbook as a step-by-step guide to prepare for an incident.

Identify your cyber incident response team.

Clarify who the key players are, outline roles and responsibilities, and clearly identify which individuals have the authority to take critical response actions. Document how to contact team members 24/7, designate an alternate for key roles, and outline a battle rhythm for how and when the team will convene and deliver updates.

Identify contacts and response service contracts for cybersecurity service providers and equipment vendors.

Keep an updated list of vendor contacts and the support they can provide if a vulnerability is identified in vendor equipment. Identify a contact person for the Internet Service Provider (ISP). If the utility has contracted with third-party service providers for incident investigation, forensic analysis, or other forms of incident response support, identify the contact person, determine the process for engaging their support, and identify the person on the Cyber Incident Response Team (CIRT) who is authorized to engage their services. Determine the expected response timelines for each partner.

Understand the system and environment.

Document where system maps, logs, and inventories are kept and maintained, along with the person who has the credentials to access them. Document access credentials and procedures for removing access or providing temporary access to incident responders.

Outline your incident reporting requirements and timelines.

Depending on the type or severity of a cyber incident, utilities may be required to report the incident to

regulatory agencies and local/state/federal officials, often within the first 24 hours of an incident, and sometimes as little as 6 hours. Determine your legal and contractual obligations to report incidents to federal/state/local officials, insurance providers, and other third parties.

Identify the response procedures the CIRT will take to investigate, contain, eradicate, and recover from a variety of different incidents.

Document procedures for investigation and documentation, incident containment actions for various types of attacks, and procedures for cleaning and restoring systems. Identify and pre-position the resources needed to preserve evidence, make digital images of affected systems, and conduct a forensic analysis, either internally or with the assistance of a third-party expert.

Identify the external response organizations—including law enforcement, information sharing organizations, and cyber mutual assistance groups—the utility might engage during cyber incident response, particularly for severe incidents that outpace utility resources and expertise.

Identify key contacts within external response organizations and build personal relationships in advance of an incident. Determine how much information to share and when. Document who has the authority to engage these organizations and at what point they should be notified.

Develop strategic communication procedures for cyber incidents.

Identify the key internal and external communications stakeholders, what information to communicate and when, and what type of cyber incidents warrant internal communication with employees and public communication with customers and the media. Develop key messages and notification templates in advance.

Define response procedures and responsibilities of the utility's legal team during cyber incident investigation and response.

Cyber incident response should be planned, coordinated, and executed under the guidance of the legal team.

The Playbook includes an outline for a cyber incident response plan, a process for response planning, and offers high-level procedures and templates that a utility can use to develop its own response plan.

2 GETTING STARTED:
Building a Cyber Incident Response Plan and Procedures

Public power utilities increasingly recognize cyber incident response as a key component in their overall cyber risk management strategy. Yet many small and mid-sized public power utilities have no formal cyber incident response plan or procedures.

Despite ever-increasing cyber protections and improved monitoring, cyber attacks are growing more sophisticated and targeted to electric utilities. A robust cyber incident response plan can improve the speed and efficiency of response actions and decisions and minimize the impact of a cyber incident on business functions and energy operations. The precise procedures, roles, and priorities for cyber incident response vary based on utility size, organization, and criticality. While each individual utility's response capabilities differ, all utilities can use the guidance in this playbook to document a cyber incident response process that can be scaled as appropriate. This section of the playbook identifies key elements that utilities should consider when developing a cyber incident response plan.

Top 10 Steps to Develop a Cyber Incident Response Plan

Whether developing a formal incident response plan or ad hoc procedures, the following steps will help utilities remove significant bottlenecks and hit the ground running in response to a cyber incident.

1. Establish a Cyber Incident Response Team (CIRT)

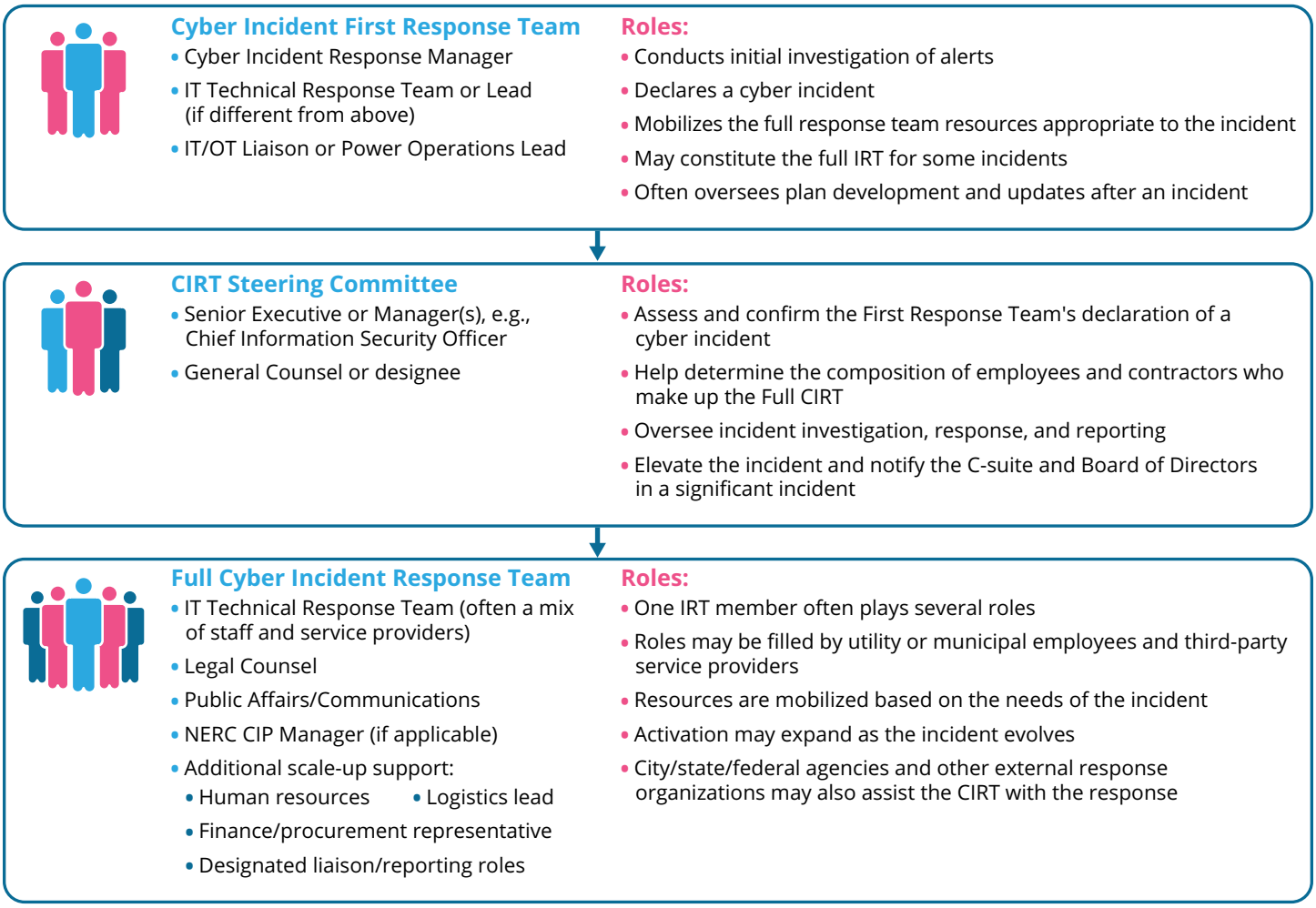
The most vital component of incident preparation is establishing a team of personnel who have the responsibility and the authority to take action during a cyber incident without delay. The CIRT includes the individuals responsible for assessing, containing, and responding to incidents, as well as those responsible for assessing the business and legal impacts, reporting incidents as appropriate, communicating to internal and external stakeholders, and engaging with industry and government response partners to coordinate information and resource sharing when needed.

Larger utilities may have dozens of staff assigned to formal technical response and crisis management roles. In contrast, incident response at smaller utilities is often led by a team of two to five IT and management staff who are familiar with the IT and cybersecurity infrastructure, and who can pull in additional representatives ad hoc from other departments as required.

The needs of the incident dictate the size of the full CIRT and which capabilities are activated. A tiered structure for the CIRT offers a flexible approach for engaging the right personnel quickly and convening a full CIRT that fits each incident's response needs. This can include:

- **First Response Team**: Includes the Cyber Incident Response Manager and other IT/OT security staff to investigate an incident.
- **CIRT Steering Committee**: Typically includes the most senior information security officer and the General Counsel (or their designees) to confirm a cyber incident and oversee response.
- **Full CIRT**: A complete list of individuals and roles that can be engaged as needed to scale-up and support response.

Tiered Cyber Incident Response Team (CIRT) Approach



Roles and Responsibilities

For many utilities, the response effort involves not only utility staff but also other municipal employees and third-party resources. Key team roles may be filled by city or state IT cybersecurity departments, system operators, legal teams, compliance officers, human resources staff, and public affairs or media relations staff. Many public power utilities also contract out cybersecurity services involved in detection and response (such as system monitoring and intrusion detection) and hire third-party, on-call service providers to assist in key areas of incident response, such as forensic analysis and incident mitigation. These third parties are members of the CIRT and should be included in cyber response planning. External federal, state, and city agencies may also be involved in the response, but are not members of the CIRT.

Particularly at smaller utilities, one person may serve in multiple roles on the CIRT. For example, the Cyber Incident Response Manager and IT technical response lead are often the same person. The human resources and logistics liaison roles may be collapsed, and several of liaison roles may be played by one person.

Small cybersecurity teams can deliver a flexible, agile response—provided roles, responsibilities, and contacts are clearly identified ahead of time. The following table identifies the matrix of roles, diverse skill sets, and responsibilities that may be required in a significant cyber incident. Consider which staff or resources may be required to fulfill these roles, recognizing that an individual may serve multiple roles within the team.

First Response Team Roles

Cyber Incident Response Manager	Manage cyber incident from detection to recovery and direct response procedures. Declare and categorize cyber incidents. Notify and liaise with senior management. Work with the CIRT Steering Committee to ensure the CIRT has the necessary personnel, resources, and skills. Requires a working knowledge of the utility's IT systems and cybersecurity capabilities.
Senior Management/ Executive	Assess the business impact of a cyber incident with SME input. Allocate resources or authorize contracted cyber incident services. Communicate with city/state/federal officials. Determine when to voluntarily engage outside support or request cyber mutual aid.
IT Technical Response (One or multiple staff from the utility and/or municipal IT security department or contracted service provider)	Investigate and analyze cyber incidents; and identify and conduct actions necessary to contain, eradicate, and recover from an incident under direction of the Cyber Incident Response Manger. Required capabilities include: • **Network Management**: Technical understanding of the utility's network to analyze, block, or restrict data flow in and out of network. • **Workstation and Server Administration**: Analyze compromised workstations and servers. • **Forensic Investigation**: Gather and analyze incident-related evidence at the direction of counsel and in a legally acceptable manner; conduct root cause analysis. • **Applications/Database Administration**: Understanding of the normal/baseline operation of enterprise applications to analyze abnormal behavior.
IT/OT Liaison or Power Operations Lead	Coordinate between IT cybersecurity staff and operations staff during cyber events that could affect operations. Assess and communicate potential impacts of a cyber incident on control systems and energy delivery; communicate impacts to the Cyber Incident Response Manager; and direct response procedures that affect energy delivery systems and equipment. Requires a working knowledge of the utility's critical operations systems (e.g., SCADA system, distribution management system).

Additional CIRT Roles (as required)

Legal Counsel	Oversee the investigation of the cyber incident. Assess the legal ramifications of a cyber incident. Ensure regulatory and contractual compliance. Ensure all response activities comply with federal and local rules and regulations. See *Section 6: Cyber Incident Response Legal Procedures*.
Communications/ Public Affairs Personnel	Support the technical response team in devising messages to appropriately communicate to all relevant stakeholder groups. Proactively communicate and quickly respond to all employee, media, and customer inquiries. Work with other utilities and APPA to coordinate messaging across the industry for significant cyber events. See *Section 5: Strategic Communication Procedures*.
NERC CIP Manager (if applicable)	Ensure incident response actions and reporting comply with NERC CIP requirements.
Human Resources	Ensure staff resources to enable 24/7 response operations as directed by the Cyber Incident Response Manager. Assist with managing any communications with employees relating to the cyber incident.
Logistics Lead	Manage all activities pertaining to logistics of cyber response (e.g., food, accommodation, workspace, equipment, building and network access, etc.).
Finance Representative	Determine the cost of an incident and appropriately allocate funds to management team.
Physical Security Officer	Manage and ensure needed physical access to on-site and off-site premises and physical protection of cyber infrastructure.
Union Liaison	Communicate with union leadership to ensure employee reporting protocols are met.
Law Enforcement Liaison	Notify law enforcement of the cyber incident, in coordination with the CIRT Steering Committee.
Liaison to Senior Executives/Board of Directors	Keep senior leadership and the Board of Directors apprised of the response to the incident, any operational or business impacts, and any internal or external communications. Share the input of the senior leadership and board with the full CIRT.
Federal Liaison	Communicate with federal response entities (e.g., MS-ISAC, E-ISAC, DHS/NCCIC, DOE, etc.) for situational awareness, regulatory compliance, incident reporting, and mitigation assistance.
Cyber Insurance Liaison	Communicate with the insurance company and ensure compliance with policy requirements.

Staffing the Cyber Incident Response Team

Consider the following factors when assessing CIRT staffing needs:

- **24/7 Availability:** Designate and train backup roles for critical staff, as incidents may occur during off-hours or vacations for lead staff. Some cyber incidents may require around-the-clock response, which can quickly tax incident response employees. Lead and backup roles may need to work in shifts, or require contract resources or service providers to supplement staff roles.
- **Cost and Training:** Utilities should account for not only compensation, but also the cost of training and maintaining cyber incident response skills, when assessing incident response planning budgets.
- **Staff Expertise:** Incident handling and mitigation often requires specialized knowledge and experience. Third-party experts can provide on-call intrusion detection, investigation, forensics, and recovery services to supplement in-house skill sets.

Build from the utility's natural disaster incident response plan when identifying the cyber incident response team. First, several response roles that are required in any type of incident (e.g., human resources, logistics, and many liaison roles) may already have clearly defined responsibilities, authorities, and personnel. Second, these plans may have accounted for staffing considerations of large events, including staffing a 24/7 response operation, compartmentalizing roles to minimize oversight from key staff, assessing response cost, and maintaining employee morale during taxing, multi-day incidents.

Ensure CIRT members have the necessary authority to act. Cyber incidents can be fast moving, requiring rapid decision-making by a small team of people with little time to seek authorization for important response activities. Consider in advance what authorities CIRT team members will need:

- Who on the CIRT has the authority to make critical decisions to contain a cyber incident, such as to isolate or disconnect key business and operational networks?
- Who is authorized to request additional support from service providers? What resource procurement processes must be followed?
- Who has the authority to report a cyber incident? Who will interface with external incident response partners (e.g., vendors, ISACs, APPA, etc.)?
- Who will ensure compliance with mandatory reporting requirements and notify government officials and regulatory bodies?
- Who will report a suspected criminal attack to law enforcement and submit mandatory paperwork to regulatory bodies?

2. Develop a 24/7 Contact List for Response Personnel and Partners

Develop and regularly update contact lists for incident response team personnel, vendors and security service providers that may be on call during an incident, and external partners that can provide aid or information at crucial junctions during response. Establishing this contact in advance can help incident managers, IT personnel, and management alert and engage resources early, even without a formal incident response plan in place. This list should contain the names, roles, contact and backup contact information, and potential alternate for each role. It should be maintained online and also in a central, offline location (e.g., physical binder, offline computer) and circulated widely among the incident response team.

Contact lists can include:

- **Internal stakeholders**:
  - Departmental leads on the incident response team (senior management, IT security, operations personnel, public affairs, legal representatives, etc.)
  - CISO and IT security department for state/local jurisdictions
- **Support contacts for all software and equipment vendors and contracted service providers**. Identify the support contact personnel, the type of support expected and contractual requirements for:
  - Critical system vendors, who can provide information on the significance of log entries or help identify false positives for certain intrusion detection signatures
  - Internet service provider (ISP), who can provide requested information about major network-based attacks, identify potential origins, or potentially block communication pathways as requested.

- Contracted security service providers for monitoring, investigation and forensics, and response, as applicable
- Insurance brokers and other legal or business resources to support business continuity

- **Key contacts or liaisons** for industry and government response partners:
  - Cybersecurity liaisons at law enforcement agencies (e.g., FBI, state/local agencies as appropriate)
  - Incident reporting and information-sharing organizations (e.g., E-ISAC, MS-ISAC, DHS NCCIC)
  - Cyber contacts at APPA and/or Joint Action Agency who can coordinate and connect resources
  - Cyber mutual assistance contacts
  - Federal response agencies (e.g., DHS NCCIC, DOE)

3. Compile Key Documentation of Business-Critical Networks and Systems

Documenting the following information is especially helpful if an incident occurs when the primary management team is unavailable, or if additional vendor support or expertise must be pulled in to manage a significant or fast-moving cyber event:

- **An inventory of the IT/OT systems and networks that support core business and operational processes can help to quickly investigate the extent of an incident and assess potential impacts**. For each application or process, identify which IT/OT assets, systems, and network connections support it. Assigning a business priority for recovery can establish the order in which systems should be restored.
- **Network Scheme** displaying the network architecture with internal network segmentation and the various gateways networks, as well as range of DMZ, VP, and IP addresses used. Network maps can help quickly orient cyber management teams.
- **Equipment and configuration inventory** of core assets in utility environment and server and network components used to deliver corporate and operational services. This inventory not only supports risk management, it enables IT personnel to quickly determine whether a newly discovered vulnerability or attack could affect the utility's equipment, the potential extent of compromise, and the processes or functions that could be affected.
- **Account permission list** to discern who has the authorization to access, use, and manage the utility network and the various systems within it. This will help IT personnel investigate and confirm unauthorized access and remove access to isolate an incident.

4. Identify Response Partners and Establish Mutual Assistance Agreements

Many utilities lack a clear strategy to engage outside resources if an incident overwhelms the cyber response resources and expertise of their cybersecurity staff and contracted cybersecurity service providers. Identifying how to engage external response organizations, signing NDAs, and reviewing legal agreements in advance of an incident can shave precious time off of incident response in a significant incident.

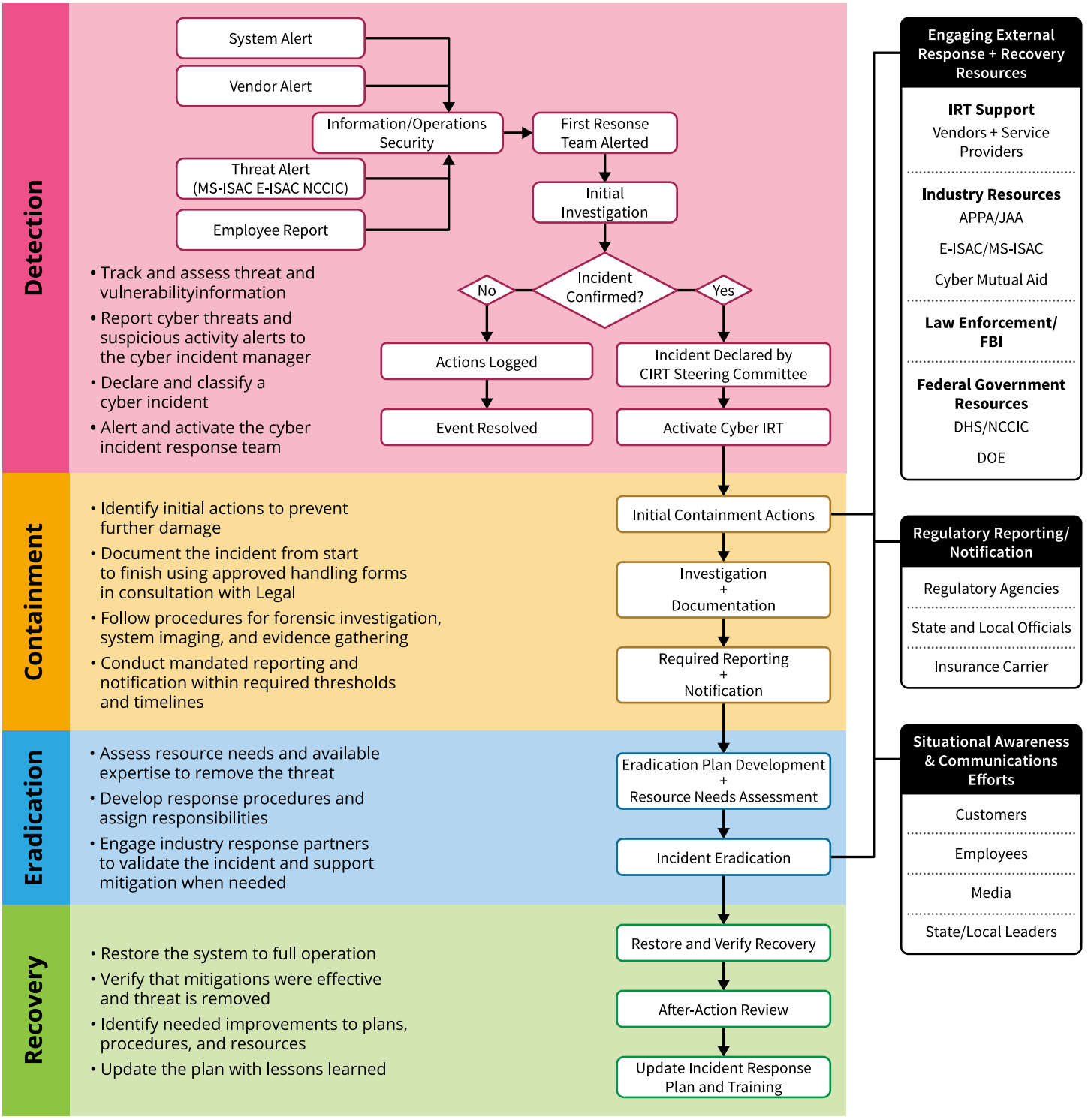
Section 3: Engaging Help **outlines a playbook for engaging industry and government partners that utilities can integrate into their incident response plans.**

5. Develop Technical Response Procedures for Incident Handling

The utility should develop a detailed list of response processes—designating which CIRT members act and when—for all phases of a cyber incident (detection and analysis, containment, eradication, and recovery). The following graphic provides a high-level overview of a public power utility's typical cyber incident response process.

See *Section 4: Digging Deeper* for guidance on an overall process flow and response steps for technical incident response.

Cyber Incident Handling Process



6. Classify the Severity of Cyber Incidents

It is helpful for utilities to have a framework to categorize the severity of a cyber incident. Using common severity levels can help the CIRT quickly mobilize the right resources based on the type of incident and convey the potential impacts when notifying internal and external stakeholders. "Sample Cyber Incident Severity Levels" on the next page provides a sample schema to categorize cyber incidents, considering the functional impact, information impact, and recoverability effort that typically characterize these incidents. The right-most column of the table shows how these levels can align with the uniform threat severity schema for national cyber incidents, developed by the United States Federal Cybersecurity Centers and commonly used among federal cyber response organizations.

Each utility should define severity levels that best reflect their design and operations. The sample severity levels use Level 1–3 to define impacts to business systems, and reserve Level 4–5 for cyber incidents that impact operational systems and may affect power delivery. At some utilities, however, losing some IT systems may disrupt the utility's ability to operate far more than losing its SCADA systems, which can sometimes be replaced by manual controls.

See "Investigate and Declare a Cyber Incident" in *Section 4: Digging Deeper* for additional guidance on assessing incident severity and declaring a cyber incident.

7. Develop Strategic Communication Procedures

Information sharing policies and procedures should be developed with input from the utility's public affairs/communications department, legal department, and senior management. The aim is to control communication flow to ensure the right information is communicated at the right time by the right personnel, through approved channels, to the right stakeholders. The nature of the incident will determine the type of communication required, however a principle of "need to know" should be respected internally.

***Section 5* provides guidance on developing strategic communication procedures for key stakeholders.**

8. Develop Legal Response Procedures

A utility's legal team must be central to its cyber incident response plan. Utilities should develop Cyber Incident Legal Response Procedures, and promptly alert the legal team of a cyber incident. To ensure compliance and preserve the utility's legal posture, the legal team should oversee and direct the incident investigation, documentation, and reporting.

***Section 6* provides guidance on the legal team's role in the Cyber Incident Response Plan.**

9. Obtain CEO or Senior Executive Buy-In and Sign-off

Review contents of the incident response plan with senior executives/general manager and obtain their buy-in with signature forms. Senior management should particularly review the roles and responsibilities of the cyber incident response team and approve the authorities of key team members during incident response.

10. Exercise the Plan, Train Staff, and Update the Plan Regularly

A cyber incident response plan on paper has little value if cyber incident responders do not understand their roles and exercise response steps regularly—ideally at least once per year. The CIRT Steering Committee should convene key members of the CIRT, train them on processes and procedures, and conduct exercises or participate in industry exercises to test the plan.

- **Test a variety of different scenarios and impacts** to identify gaps in procedures or staff capabilities. (*Section 7* has sample incident scenarios at multiple severity levels that can help develop and test response procedures).
- **Conduct abbreviated exercises during plan development** to help generate discussions on roles, authorities, and response procedures. In between exercises, conduct drills with small teams of employees to reinforce their roles and identify training needs.
- **Practice incident documentation during exercises**, including using incident handling forms, preserving forensic images, and accessing and investigating logs.
- **Review and update the incident response plan** on an annual basis (especially contact sheets) and as part of any post-incident review.

Sample Cyber Incident Severity Levels

Operational System (OT) and Business Impact	Level 5	**Cyber or cyber-physical event that directly impacts power delivery at one or multiple utilities**	Utility can no longer provide a critical operational service to all or a subset of users	Critical electric infrastructure information was compromised	Unpredictable; additional resources and outside help are needed	Poses an imminent threat to the provision of wide-scale critical infrastructure services
	Level 4	**Compromise of network or system that controls power generation and delivery and could lead to an outage at one or multiple utilities**	Utility can no longer provide a critical business service to all system users or can no longer provide a critical operational service to a subset of users	Critical electric infrastructure information was compromised	Unpredictable; additional resources and outside help are needed	Likely to result in a significant impact to the public health or safety, national security, economic security, foreign relations, or civil liberties
Business System (IT) Impacts	Level 3	**Compromise or denied availability to a business-critical enterprise system or service (e.g., corrupt or destroy data)**	Utility can no longer provide a critical business service to a subset of system users	Sensitive, PII, or proprietary information was accessed, changed, exfiltrated, deleted, or made unavailable	Unpredictable; additional resources and outside help may be needed	Likely to result in a demonstrable impact to the public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
	Level 2	**Compromise of security to non-critical enterprise business systems**	Minimal effect; the utility can still provide all critical business services to all users, but has lost efficiency or lost some non-critical services	Non-PII or proprietary information was accessed or exfiltrated	Predictable with existing or additional resources	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
	Level 1	**Suspected security threat or isolated incident with minimal impact (e.g., unidentified server on network, successful phishing attempt with no loss of data)**	Minimal effect; the utility can still provide all critical services to all users, but has lost efficiency	Sensitive information at-risk but not exfiltrated	Predictable with existing or additional resources	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence
	Level 0	**Notification of suspicious behavior**	No effect to the organization's ability to provide all services to all users	No information was exfiltrated, changed, or deleted		Unsubstantiated or inconsequential event

Cybersecurity Best Practices to Support Effective Response

Many public power utilities are taking steps to improve their cyber risk management capabilities in a host of areas. Many of the risk management activities in the APPA Cybersecurity Scorecard and Cybersecurity Roadmap not only support strong cybersecurity, but promote an effective response when a cyber incident occurs. Examples of these best practices include:

- **Establishing a process** for identifying and evaluating cybersecurity risks that can compromise energy delivery operations.
- **Developing and enforcing** strong access control policies and procedures for requesting, approving, providing, and revoking access for employees, devices, and entities.
- **Identifying sources** of threat and vulnerability information and creating a process for collecting, cataloging, and addressing information collected from internal and external sources.
- **Maintaining network**, systems, and applications security by training IT staff on in-house security standards. Employees and contractors are a major organizational security risk.
- **Creating a policy** that specifies where and how long to retain system logs such as firewall, intrusion detection system, and application logs. Older logs can show evidence of reconnaissance or intrusion information, especially if an incident is not discovered for weeks or months.
- **Conducting regularly scheduled training** to educate and test employees' cybersecurity awareness. A cyber attack may target a utility employee (e.g., spear phishing) to access unauthorized information, gain credentials, or spread malware.
- **Improving communication** and coordination among IT cybersecurity and OT staff. OT staff should understand cyber technical requirements, as cyber incidents affecting operational systems can threaten energy delivery.
- **Ensuring equipment is purchased** from a reputable vendor with reliable products and regularly patching security flaws and vulnerable configurations.

3 ENGAGING HELP:

Activating the Response Team and Engaging Industry and Government Resources

Activate the Cyber Incident Response Team

Once the Cyber Incident Response Manager has identified a cyber incident, the CIRT Steering Committee should confirm the incident and work with the First Response Team to convene a full Cyber Incident Response Team. The make-up of the CIRT will initially depend on the scale of the incident. A low-severity incident may require only the IT technical support team, public affairs, and legal representatives while the incident is contained and investigated. High-severity incidents may require immediately convening all representatives on the CIRT to begin standing up a round-the-clock incident response operation.

The utility's cyber incident response plan should outline the process to activate the response team and the logistics to support it. The CIRT should determine how frequently the team will meet and be briefed, how updates will be delivered (e.g., email, in-person meetings), and backup communication methods if the primary systems are affected by the cyber incident. Consider designating and pre-staging the following for CIRT coordination:

- A dedicated "war room" for central communication and coordination and a dedicated conference bridge for team members to meet.
- Encrypted messaging systems or other secure systems for incident communication.
- Dedicated cell phones for CIRT members for off-hour support and onsite communications.
- Printed copies of incident response procedures, contact lists, and incident handling forms.
- Secure storage facility for securing evidence and other sensitive materials.
- Secure file system, application, or database with access restrictions to store sensitive incident handling forms and information.

Engage Expert Response Resources

Few utilities, regardless of size, can manage a significant cyber incident with in-house resources alone.

Many public power utilities employ third party support staff to supplement in-house cybersecurity, monitoring, and response capabilities. When an incident requires expertise, tools, or capabilities beyond the resources of utility staff, vendors of affected equipment and contracted cybersecurity service providers are often the first line of contact for cyber incident response, as their team may be equipped to help the utility assess and respond to the threat.

In a major cyber incident, utilities will likely need to engage a bevy of external response organizations: from law enforcement to information sharing organizations and industry associations. In the case of a highly sophisticated attack or one that disrupts electricity, smaller to medium sized public utilities may not possess the necessary expertise, staff capacity, or resources to effectively mitigate an incident. Processes exist to request cyber mutual assistance from utilities across the industry, as well as mitigation support from federal incident response teams.

This section provides a process flow for reporting and escalating cyber incidents both internally and externally. The following pages also describe external response organizations and offer guidelines for when to engage them and how they can support incident, investigation, response, and mitigation.

Benefits of Early Incident Notification

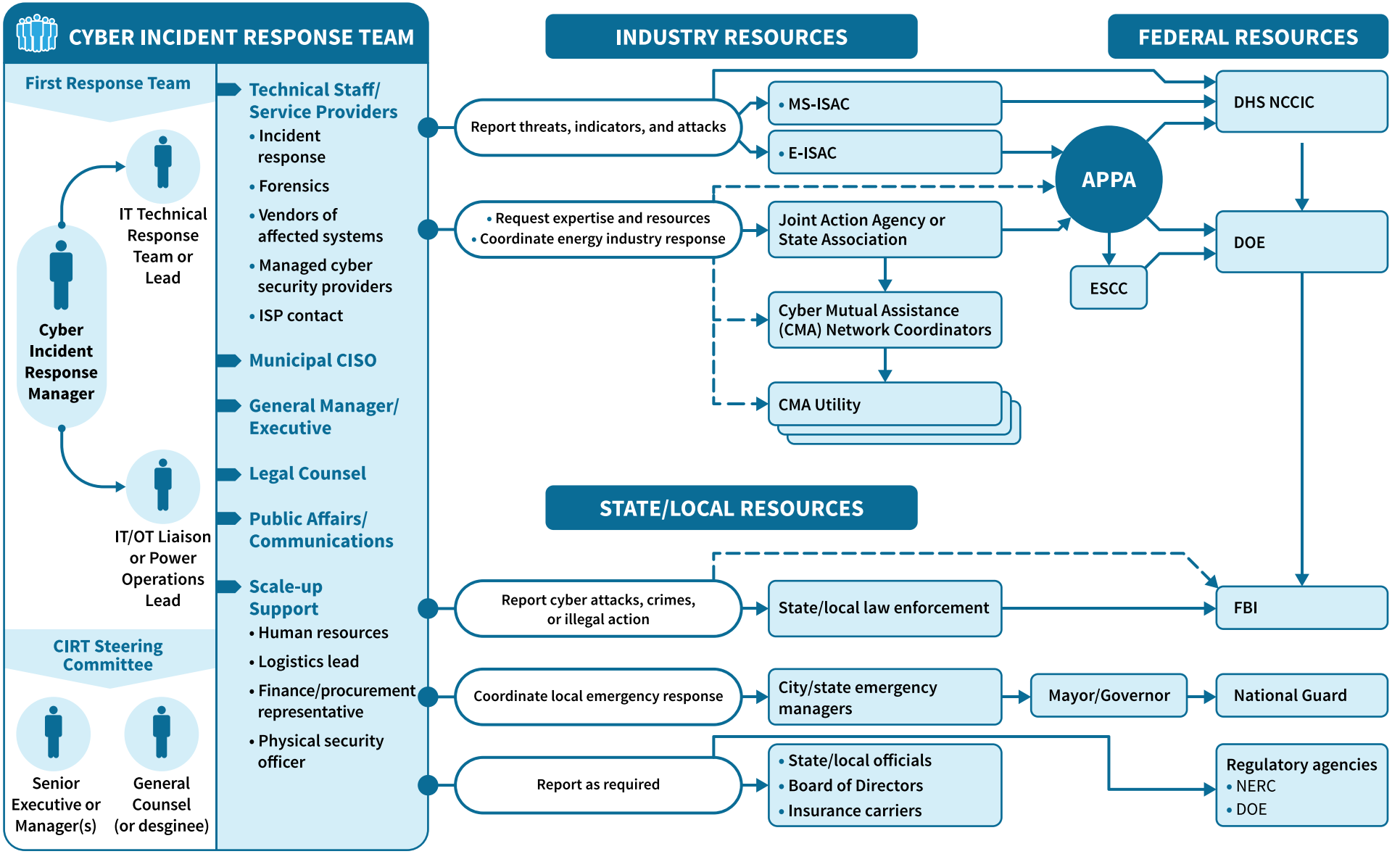
- **Correlating incidents across industry to identify coordinated attacks or attack trends**. Reporting suspected or confirmed incidents to the E-ISAC and MS-ISAC early allows these partners to analyze the report against other reports and threat information, allowing for early detection of a more coordinated, widespread attack.
- **Mitigation measures and expertise**. Organizations may be able to recommend mitigation steps for similar cyber incidents, or conduct analysis of malware or threat signatures to identify ways to mitigate the incident.
- **Incident investigation support**. Several external response groups can support the utility's forensic analysis and investigation of an incident, either remotely or onsite.
- **Readying response and coordination resources**. Notifying external response groups early can help kickstart cross-industry coordination, prepare response teams for potentially severe incidents, and support messaging coordination among response partners.

Things to Consider before Reporting Incidents

- Consult with legal counsel before making any notification outside of the utility. Determine and authorize acceptable circumstances for notification in advance.
- Review information protections and ensure non-disclosure agreements are in place before voluntarily sharing information. Work with the legal team to review and sign the non-disclosure agreements (NDAs) with the Cyber Mutual Assistance Program in advance. Review the protections offered by the ISACs and government agencies to understand how information will be protected.
- Clearly identify what information about the incident can be shared with others. Both the E-ISAC and MS-ISAC will verify what information the utility will allow them to share with partner networks and how the information will be scrubbed for anonymity.
- Designate liaisons to communicate with external response groups where possible to avoid overloading the Cyber Incident Response Manager. Prepare talking points in conjunction with legal, communications, and other CIRT members, and require liaisons to communicate only what is in the talking points.
- Identify contacts and build relationships with law enforcement in advance. Understand their expectations for information and access if the utility reports a cyber crime, and how to coordinate with law enforcement during response and recovery.
- Disclose if you notify more than one law enforcement agency (e.g., FBI) or other government agency (e.g., DHS, DOE) to avoid jurisdictional or interagency conflicts. Track and share the case number and contact person assigned.

The following diagram presents a possible "call tree" and process flow for activating the Cyber Incident Response Team and engaging additional response resources as a cyber incident escalates in severity. Keep in mind the operational impacts do not have to be severe for a cyber incident to be considered significant. Industry-wide communication and coordination may be required for a more minor cyber incident if, for example, it affects multiple utilities or attracts national media attention.

Cyber Incident Resource Activation Tree



Overview of Response Partners

Information Sharing and Analysis Center (ISAC)	**Electricity ISAC (E-ISAC)** • The E-ISAC provides a voluntary, secure, confidential platform to report cyber threats and incidents in the electricity sector. The Watch Operations team gathers, analyzes, and shares security information provided by vetted electricity organizations and other watch centers; coordinates incident management; and communicates mitigation strategies. All information shared with the E-ISAC is protected from regulators (e.g., FERC, NERC). • All incidents submitted to the E-ISAC Watch Operations team or to the E-ISAC portal are logged/ticketed to facilitate trend analysis. The Watch Operations team conducts initial analysis of the information, follows up with the provider, and takes the appropriate action.	• Report suspected or confirmed cyber incidents, indicators, vulnerabilities, unauthorized changes to hardware/ firmware/software, compromised passwords, malware, denial of service attacks, or website defacement. • Report any malware or unauthorized activity within an IT or OT environment with direct impact to operations.	• Issue cyber/ physical bulletins on actionable threat and vulnerability information and indicators. • Host monthly member briefings.	• Collect, analyze, and coordinate action on collected cyber incidents. • Collect and share remediation and mitigation guidance among affected members. • Connect members to cybersecurity services such as malware reverse engineering and analysis of indicators of compromise.	• Coordinate incident response, mitigation, and information sharing among the ESCC and federal response partners (DOE, DHS, FBI).
Information Sharing and Analysis Center (ISAC)	**Multi-State ISAC (MS-ISAC)** • MS-ISAC is a no-cost cybersecurity resource for state, local, tribal, and territorial government entities that provides real-time monitoring, threat analysis, and early warning notifications through their 24/7 Security Operations Center (SOC). • Also offers a paid network monitoring and cyber response service to members, including 24/7 system monitoring through their "Albert" intrusion detection system (which leverages the Suricata IDS engine) and triage, investigation, and response support for detected incidents.	Report suspected or confirmed cyber incidents, indicators, unauthorized changes to hardware/firmware/ software, compromised passwords, malware, denial of service attacks, or website defacement.	• Issue cyber alerts on vulnerabilities and attack trends. • Monitor reported incidents and IDS alerts from the "Albert" IDS to identify and correlate attacks.	• Issue alerts on active threats. • Provide incident response and remediation planning, and help coordinate local and state resources. • Response teams can remotely help perform triage, locate the root cause, and remediate incidents.	• Coordinate incident response, mitigation, and information sharing among federal response partners and incident watch centers.

Overview of Response Partners *(continued)*

Industry Support	**Joint Action Agency/ State Association** Joint Action Agencies (JAA)—and similar state or regional associations of public power utilities and municipalities—can help coordinate cyber incident response among members or with the wider industry. Some JAAs coordinate and manage requests for cyber mutual assistance from members.	Share information or request support throughout incident response.	• JAAs may offer cyber resources such as training, commercial cyber tools and testing at discounted rates, and third-party network monitoring solutions.	• Coordinate information and resource sharing among members. • Coordinate with APPA to connect members to response resources.	
Industry Support	**Cyber Mutual Assistance (CMA) Program** The ESCC's CMA Program is a voluntary program that helps utilities confidentially request cyber resources and expertise from energy utilities across the nation. Participating utilities sign a mutual non-disclosure agreement (NDA), send resource requests to the CMA network or to individual utility coordinators, and reimburse expenses for aid provided, similar to traditional mutual aid agreements. *See "Cyber Mutual Assistance Process" on page 23 for more information, and see Appendix D for a sample NDA.*	Request information, expertise, and virtual/ onsite response support from utility peers during incident investigation, mitigation, and recovery.	• Utilities designate a coordinator and review/ sign the NDA. CMA Program convenes participants to plan and coordinate response processes and share sensitive information.	• CMA Coordinator Committee responds to requests for cyber mutual assistance from participating utilities and shares information about active threats.	• Coordinators work with the ESCC and APPA to coordinate requests and streamline information and resource sharing.

Overview of Response Partners *(continued)*

Industry Support	**American Public Power Association (APPA)** APPA represents public power utilities on the ESCC, coordinates messaging with the media during cyber events, and serves as a liaison with the federal government for public power members. Reporting a cyber incident early can help the Association prepare to engage federal resources, coordinate an industry-wide response, and help utilities confirm if an incident is isolated or may be part of an attack targeting utilities or vendor systems.	Alert the Association early in an incident that may require industry coordination so the response team can begin gathering information and preparing partners.	• Maintain contacts with utilities and JAAs. • Offer a host of cybersecurity tools, training, and guidance.	• Serve as a liaison to connect affected members to industry and federal response resources. • Provide guidance on industry coordination during an incident. • Work with the ESCC to assist a utility with traditional and social media response if needed.	• Represent public power utilities to coordinate an industry-wide response. • Share and coordinate resource needs with federal response agencies.
Industry Support	**Electricity Subsector Coordinating Council (ESCC)** The ESCC is a council of utilities and trade organizations that serves as the principal liaison with federal leadership to prepare for and respond to national-level incidents or threats.	A utility member or the APPA can activate conference calls with industry partners for information sharing and response coordination before or during an incident.	• Coordinate with industry and federal partners to improve incident planning and preparation.	• Activate the ESCC Playbook when requested by a utility or APPA to coordinate industry messaging and response.	• Connect affected utilities to share information, collect mitigations, and proactively communicate with the media.
Law Enforcement	**Local/state law enforcement agency** State and local law enforcement offices may have a cyber division that can offer expertise or guidance on documenting and preserving evidence for a forensic investigation.	Report suspected cyber crime, including any illegal intrusion, attack, or espionage, or if sensitive data is hacked, stolen, or held ransom.	• Offer guidance on evidence gathering and handling procedures. (Utilities should build personal contacts during steady-state).	• Support forensic investigation and evidence documentation. • Prosecute cyber crimes.	• Coordinate investigation with other agencies.

Overview of Response Partners *(continued)*

Law Enforcement	**FBI Field Offices** The FBI conducts cyber threat investigation; supports cyber prosecutions; and supplies, supports, and coordinates intelligence analysis with federal agencies and the intelligence community through the National Cyber Investigative Joint Task Force (NCIJTF).	Same as above, particularly for sophisticated or serious incidents targeting critical utility operations. State law enforcement may also escalate to the FBI.	• Cyber threat investigations and intelligence analysis to thwart significant threats.	• Contact known targets of classified cyber threats and attacks.	• Investigate and provide expertise to remediate significant cyber attacks on energy infrastructure. • Coordinate with DHS and DOE to support recovery of affected utilities.
Federal Response Support	**DHS National Cybersecurity and Communications Integration Center (NCCIC)** NCCIC is a 24/7 cyber situational awareness, incident response, and management center with the primary aim of reducing cybersecurity risks across critical infrastructure by partnering with the intelligence community and law enforcement agencies as well as coordinating efforts between government bodies and control systems owners, operators, and vendors.	Individuals or ISACs can report suspected or confirmed cyber incidents, indicators, phishing attempts, vulnerabilities, and discovered malware.	• Provide actionable alerts and conduct analysis on malware and vulnerabilities.	• Coordinate the responsible disclosure of threats, vulnerabilities, and mitigations.	• Hunt and Incident Response Teams (HIRTs) can provide onsite support to entities requesting help to investigate, remove adversaries, and restore operations during severe incidents.
Federal Response Support	**DOE Emergency Response Support** Provides technical expertise and assistance to support response and recovery to incidents that affect critical energy infrastructure.	Report severe incidents that meet reporting criteria. *See Appendix C.* APPA and the ESCC can help share member information and resource needs with DOE.	• Coordinate with the ESCC for incident response planning and conduct exercises.	• Coordinate information and resource sharing with industry and government.	• Collect incident reports and coordinate information and resource sharing with industry and government.

Cyber Mutual Assistance Process

For decades, electric utilities have offered critical aid to each other during an emergency event by providing crews, equipment, and resource capacity at cost. The public power Mutual Aid Network has developed a coordinated process that enables utilities to efficiently share resources and restore power faster when natural disasters hit. A national mutual aid agreement, signed by more than 2,000 public power and rural electric cooperatives, provides the framework for electric utilities to formally request support from other utilities during a natural disaster.

Hower, cyber incident response requires a vastly different mix of personnel, expertise, and equipment resources. The Electricity Subsector Coordinating Council (ESCC) has used the mutual aid model to develop a process for utilities to share resources during cyber incident response.

The ESCC's Cyber Mutual Assistance (CMA) Program is a voluntary, no-cost program that helps utilities engage cyber resources and expertise from energy utilities across the nation. All organizations that provide or materially support the provision of generation, transmission or distribution electric or natural gas service are eligible to sign up for this program. Participation in the program and responses to requests for assistance are voluntary. There is no cost for organizations to participate in CMA (other than the reimbursement of the expenses incurred in providing emergency cyber assistance).

To participate in the CMA Program, each participating entity must:

1. **Sign a Mutual Non-Disclosure and Use of Information Agreement (NDA)**, which will protect the confidentiality of all information shared between entities participating in the CMA Program.
2. **Designate a Cyber Mutual Assistance Coordinator (CMA Coordinator)** who will serve as the primary contact for the program. The Coordinator must be a senior-level employee with the authority to act on behalf of the participating entity it represents.

The program can be triggered at any time, by any of the entities participating in CMA. **When emergency assistance is needed, a request can be sent directly to another participating entity (or entities) or to the Coordinator Committee.** Proxies such as joint action agencies (JAA) or larger utilities can also be designated to represent smaller utilities in meetings and response activities. Proxies must sign the NDA and cannot make commitments on behalf of the utility, but they can help coordinate requests and information sharing.

Requests for assistance may be made in connection with a cyber emergency or in advance of a threatened or anticipated cyber emergency. There is a playbook on the member portal that provides step-by-step guidance on requesting and providing aid.

There is no obligation for a smaller entity to commit resources. The program enables smaller utilities with finite resources to draw upon the expertise of their larger counterparts. The assistance provided by outside experts is intended to be advisory in nature and provided on a short-term basis. It may include services, personnel, and/or equipment. Depending on the incident, the assistance can be provided remotely by WebEx, which eliminates the need for travel.

Furthermore, the CMA Program is not only used to respond to a cyber emergency, but also on a proactive basis when significant cyber threats or potentially critical cyber system vulnerabilities have been identified by industry and government partners.

Signing the NDA and reviewing legal agreements in advance of an incident can shave precious time off of incident response—particularly during a significant cyber incident that overwhelms the cyber response resources and capabilities of utility staff and service providers.

Key Contacts

State and Local Law Enforcement [To be updated by individual utility]	**FBI Cyber Task Force Field Offices** Find your Field Office: *www.fbi.gov/contact-us/field* Report individual instances of cyber crime to the Internet Crime Complaint Center: *www.ic3.gov*
E-ISAC Contact Information • Operations Desk: 202-400-3001 • 24-Hour Hotline: 404-446-9780 • Email: operations@eisac.com • Portal: *www.eisac.com*	**MS-ISAC Contact Information** **Security Operations Center (SOC) can be contacted 24/7:** • Phone: 866-787-4722 • Email: *soc@msisac.org* **Computer Emergency Response Team (business hours ET):** • Phone: 518-266-3460 • Email: *Valecia.Stocchetti@cisecurity.org*
CMA Contact Information **Carter Manucy (FMPA)** • Email: *Carter.Manucy@fmpa.com* **Kaitlin Brennan (EEI)** • Phone: 202-508-5517 • Email: *kbrennan@eei.org* **Nathan Mitchell (see APPA)**	**APPA Contact Information** **Michael Hyland** • Phone: 202-467-2986 (office) • Phone: 202-731-1810 (cell) • Email: *MJHyland@PublicPower.org* **Nathan Mitchell** • Phone: 518-266-3460 (office) • Phone: 202-731-1851 (cell) • Email: *NMitchell@PublicPower.org*
JAA/State Association Contact Information [To be updated by individual utility]	**NCCIC Contact Information** **NCCIC watch floor can be contacted 24/7:** • Phone: 888-282-0870 • Email: *ncciccustomerservice@hq.dhs.gov* **Submit reporting forms via the following secure web forms:** • *Incidents* • *Indicators* • *Phishing* • *Vulnerabilities* • *Malware Artifacts*
NERC-CIP Event Reporting **Submit Event Reporting Form (EOP-004 Attachment 2) or DOE-OE-417 form via one of the following:** • Email: *systemawareness@nerc.net* • Fax: 404-446-9770 • Phone: 404-446-9780	**DOE Event Reporting** **Submit DOE-OE-417 Event Reporting Form (*see Appendix C*) via one of the following:** • Online: *www.oe.netl.doe.gov/OE417/* • Fax: 202-586-8485 • Phone: 202-586-8100

4 DIGGING DEEPER:

Technical Response Procedures for Detection, Containment, Eradication, and Recovery

This section contains guidelines and considerations for utilities as they develop detailed technical response procedures for the key phases of incident response.

Phases of Cyber Incident Response

- **Preparation** – Includes development of the cyber incident response plan and procedures for the remainder of the phases. (Planning and preparation steps are covered in *Section 2: Getting Started*. See *Appendix A* for an Incident Response Plan Outline.)
- **Detection, Investigation, and Analysis** – Includes procedures for alerting and detection, escalation, declaration of a cyber incident, incident classification and prioritization, and investigation of the incident.
- **Containment** – Includes activating the Cyber Incident Response Team, conducting initial containment actions, documenting the incident, establishing procedures for evidence gathering and handling, and conducting required incident reporting.
- **Eradication** – Includes developing response solutions, assessing resource needs, engaging external resources and response organizations, and following a response plan to eradicate the threat.
- **Recovery** – Includes restoring the system to full operation and verifying that mitigation actions were effective. Also includes reviewing response actions, documenting lessons learned and updating the plan.

Detecting and Analyzing a Cyber Incident

One of the most challenging parts of the incident response process is determining whether an incident has occurred, and if so, the type and magnitude.

Incident alerts typically come in two forms: *precursors* or *indicators*. A precursor is a sign that an incident may occur in the future, while an indicator is a sign that an incident may have occurred or is currently occurring. Indicators are far more prevalent than precursors. Examples are listed below:

- A network administrator notices uncommon fluctuation in network traffic flows
- An antivirus software alerts host upon detection of malware infection
- An application records multiple failed login attempts from an unfamiliar remote system

It is important to understand common attack vectors and develop a clear process for identifying and reporting cyber alerts to the information or operations security team, who can analyze them and alert the Cyber Incident Manager to potential incidents.

See *Appendix A: Cyber Incident Response Plan Outline* for the definitions of a cyber incident versus a cybersecurity event.

External/Removable Media	An attack carried out from removable or external device	An infected USB drive spreads malicious malware across network
Attrition	An attack that uses brute force techniques to compromise systems, networks, or applications	Continuous attack

Web	An attack carried out from website or web-based application	Website installs malware on workstation
Email	An attack carried out through a phishing email with a malicious link or attachment	The body of an email message from known address contains link to malicious website
Impersonation	An attack that inserts malicious processes into something benign	Rogue wireless access points
Improper Usage	Attack stemming from user violation of utility's usage policies	Employee installs file-sharing software
Loss or Theft of Equipment	Loss or theft of proprietary device used by organization	Stolen workstation provides attacker access to sensitive customer data

Establish a Clear Process for Identifying and Reporting Cyber Alerts

Attack precursors and indicators can be identified through several channels, including suspicious activity reported by utility employees, alerts from intrusion detection systems and other monitoring systems, review of system logs, and from threat/vulnerability databases. The team should have a process for reviewing and escalating alerts for further investigation.

Personnel Detection

Identify and train all staff on reporting mechanisms for suspicious activity or other indicators, such as a help desk phone number, email address, secure web form, or instant messaging system to report incidents to the information security team. Every member of utility organization should be aware of reporting procedures if they observe something abnormal on their computing devices.

Detection Software and Monitoring Systems

Develop a system for processing and analyzing alerts from monitoring software or systems, including:

- Intrusion detection and prevention systems, which can identify and record suspicious events, and log critical data to investigate an incident (e.g., date and time of suspected intrusions, source and destination IP addresses).
- Antivirus and antispam software that monitors networks and scans files for various forms of known malware.
- Third-party security services that monitor real-time system traffic to detect potential threats or investigate alerts.

System Logs

Reviewing logs—including operating system, service, and application logs; network device logs; and logs of network flows—can identify network trends and alert employees to suspicious behavior, or help the response team correlate events to verify an incident. Logs provide great value during incident response, as they can provide a record of attacker activity, such as connection attempts, accounts accessed, and what actions took place on critical systems.

Cyber Alerts

Monitoring alert databases for new vulnerabilities and exploits can alert the team to potential attack vectors (like newly discovered vulnerabilities) and help identify attack indicators to monitor for (such as IP addresses and behaviors). External response entities such as the E-ISAC, MS-ISAC, and US-CERT/ICS-CERT provide threat alerts on newly discovered vulnerabilities, attack methods, or attack indicators (*see the following table*).

Sources of Cyber Threat Alerts

The DHS **National Cybersecurity and Communications Integration Center (NCCIC)** analyzes cyber threats, vulnerabilities, and exploits and disseminates cyber threat alerts through two channels:

- **US-CERT** alerts focus on common computing systems and devices
- **ICS-CERT** alerts focus on industrial control systems, like SCADA systems

MS-ISAC provides real-time monitoring, threat analysis, and early warning notifications to subscribed state, local, tribal, and territorial government members.

E-ISAC serves as the primary security communications channel for the electricity industry. E-ISAC analyzes member-provided incident reports and shares alerts and mitigation strategies with members.

See *Section 3: Engaging Help* for more on what these services offer utilities during steady state and incident response.

Investigate and Declare a Cyber Incident

The utility should have clear processes in place to rapidly notify the Cyber Incident Response Manager of a cyber threat, and provide the response manager with the authority to identify, declare, and escalate a cyber incident.

Discerning actual security incidents from the many alerts and indicators can be a challenge. Intrusion detection systems may produce false positives, while employee reports of suspicious behavior and emails often do not result in actual compromise.

Before engaging the CIRT Steering Committee to convene the Cyber Incident Response Team, the Cyber Incident Response Manager may initially stand up a First Response Team who can accurately analyze and confirm an incident. This team primarily includes the Cyber Incident Response Manager and IT technical support staff.

The First Response Team can perform an initial analysis to determine which networks, systems, or applications are affected; the access vector and nature of any intrusions; and any known information about the root cause or threat actor behind the incident. This information will allow the incident response team to categorize and prioritize the incident, and identify and take appropriate actions.

Incidents should not be handled on a first-come, first-served basis, but rather prioritized based on functional impact of the incident, information impact of the incident, as well as recoverability from the incident.

- **Functional Impact**. Cyber attacks may impact the business and operational functionality provided by the IT and OT systems. The incident manager should consider how the incident will impact affected systems not only in the immediate time frame but also looking ahead to the future if the incident is not immediately contained.
- **Information Impact**. Incidents may compromise sensitive and proprietary information. The incident manager should consider how data exfiltration will not only affect the utility's overall mission but also that of partner organizations as well.
- **Recoverability from the Incident**. The time and resource expenditure in handling and recovering from an incident is primarily dependent on the scale and nature of incident. The incident manager should carefully weigh the effort necessary to fully recover from an incident against the value the recovery effort will create.

Once an incident is confirmed, the Cyber Incident Response Manager should categorize the severity of the incident and engage the CIRT Steering Committee to confirm the severity level and convene the full CIRT at the appropriate scale for incident severity. The CIRT should engage in investigative activities at the direction of legal counsel.

NIST's *Computer Security Incident Handling Guide* provides the following categories for functional impact, information impact, and recoverability effort.

None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of customers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Containment and Eradication

Conduct Initial Containment Actions

The Cyber Incident Response Manager and technical staff from the cybersecurity team will evaluate the incident and identify initial actions needed to contain the incident and prevent its spread. The team should conduct a full forensic investigation with the assistance of an expert forensic investigator, as appropriate, to determine the root cause of the incident and document attack pathways before taking extensive mitigation actions. Containing the incident should focus on preventing further damage, such as disconnecting affected devices from the internet to isolate a breach. Before taking any steps, the team should assess how their actions could impact investigation.

Experts recommend avoiding immediate actions that might compromise investigation or recovery, such as:

- **Shutting down servers and systems**, as this clears the temporary memory that can provide valuable information about the incident.
- **Cutting off a server from the internet** as it may be difficult to determine the extent of compromise if the server is disconnected from its control server.
- **Restoring affected systems from a backup** until the team can verify that backups have not been compromised.
- **Reinstalling on the same server or device without a forensic copy or image**, as this can destroy or override vital evidence.

Carefully Document the Incident

At the direction of legal counsel, begin recording detailed and precise information about a suspected incident immediately, and continue updating incident documentation througout response. The Cyber Incident Response Manager should coordinate with the team to gather the following information, which will help document the response throughout the incident, brief the CIRT or other stakeholders, and conduct required reporting or other notification:

What to Document

- The type of the incident
- The date and time of the incident
- If the incident is ongoing
- How the incident was discovered and the personnel who discovered it
- Affected devices, applications, or systems
- Current or anticipated impacts of the incident, both inside and outside the organization
- The type and sensitivity of data stored in affected systems
- Any mitigation measures planned or already taken
- Logs or other records of the incident
- List of stakeholders already contacted or other resources engaged
- Organization and incident response team points-of-contact (POC) details

Secure internal communication channels with encrypted email and chat messaging capabilities may be used to direct internal actions and disseminate information on a need-to-know basis. Only some of these details will be shared with any given stakeholder. The information included in any reports to law enforcement or when complying with legal or regulatory reporting requirements will vary depending on the circumstances.

Maintain incident information records using a secure application or database. Access to incident records should be restricted due to the sensitive nature of the data.

Incident handling form templates can be found in *Appendix B.*

Establish Evidence Gathering and Handling Procedures

The cyber incident IT support team should begin conducting a full forensic investigation at the direction of legal counsel prior to incident eradication. This is necessary for the utility to understand the full nature

and magnitude of an incident, identify pathways and actions of potential intruders, and determine how to completely remove the threat. Preserving, securing, and documenting evidence during this investigation is necessary for law enforcement to investigate and prosecute criminal attacks that steal sensitive data or malicious attacks that target energy operations.

The CIRT should meet with law enforcement agencies and legal staff to develop appropriate evidence handling procedures in advance of an incident. Some utilities may contract with third-party service providers to conduct a forensic investigation. The MS-ISAC also offers some remote support for forensic analysis for its members.

Evidence Preservation Practices

Incident handlers commonly recommend the following procedures:

- Preserve affected system log files such as firewall, VPN, mail, network, client, web, server, and intrusion detection system logs.
- Work with forensic experts to dynamically image all affected systems before disconnecting to preserve memory images, which can help identify sophisticated attack techniques that do not "write" to the hard drive. Memory images and logs are critical to identify the origin of an attack and what data may have been accessed or lost.
- Avoid probing affected computers or systems unless directed by a forensic expert, as this could alter evidence or alert hackers that their activity has been detected, which might cause them to conceal their tracks or cause further system damage.
- Law enforcement agencies may request original hard drives as evidence, requiring the team to replace drives with a new system image.
- Store evidence and incident records in a secure, central location. Clearly document how evidence was preserved and which individuals have handled all evidence throughout the incident.

The utility can contact the MS-ISAC for guidance on forensic investigation and documentation, and can request support or guidance from partner utilities. Local, state, and federal law enforcement agencies can provide guidance on preserving evidence or even support onsite investigation in a severe incident. See *Section 3: Engaging Help* for guidance on engaging federal and industry organizations during cyber incident response.

Pre-Staging Equipment for Forensic Analysis

To prepare for incident investigation, consider pre-staging tools and equipment for forensic analysis:

- A designated forensic workstation and blank, removable hard drives to create disk images, preserve log files, and save other relevant incident data.
- Spare or virtual workstations, servers, and networking equipment to restore backups, test malware, etc.
- Dedicated laptops installed with digital forensic software to analyze disk images and packet sniffers/protocol analyzers to capture and analyze network traffic.
- Evidence gathering accessories, such as incident handling forms, chain of custody forms, evidence storage bags/tags, and locked evidence storage boxes.

Report the Incident as Required by Regulations and Contracts

Public power utilities may be required to report an incident or intrusion to local, state, or federal organizations—often within the first 24 hours of discovery—depending on the type of incident, whether personal or proprietary data was exposed, and the type of assets impacted. Immediate reporting requirements typically include:

- **State or Local Laws or Regulations**: Laws or regulations within your jurisdiction may require that cyber incidents at public power utilities be reported to the chief information officer with the state or city, to the mayor or governor, or to other entities within a certain time frame. These policies and reporting requirements should be included in the utility's incident response plan. Other regulations may require the utility to take certain actions, such as notifying employees or customers about data breaches, within a specified period of time following incident discovery.

- **Cyber Insurance Contract Requirements (if applicable)**: Cyber liability insurance typically covers costs associated with compromised data and, in some cases, physical damage. Engage the cyber insurance representative and review policies before responding to an incident, as policies may dictate certain response actions (e.g., using only approved incident response vendors, notifying law enforcement, or using prescribed evidence gathering processes). Comply with insurance policy notice requirements to preserve the possibility of obtaining coverage for any losses associated with the incident.
- **NERC Regulations for Reporting Incidents that Impact Bulk Power System Assets**: The IRP should reference the utility's separate North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Incident Response Plan and include a process for engaging with the NERC CIP Manager, if applicable.
- **Department of Energy (DOE) Regulations for Reporting Incidents Impacting Operations or Power Adequacy/Reliability**: DOE has established mandatory reporting requirements and timelines for a variety of electric emergency incidents, including the following cyber events:
  - Within six hours: Report cyber events that could potentially impact power adequacy or reliability
  - Within one hour: Report a cyber event that causes operations interruptions

Electric utilities that operate as reliability coordinators or balancing authorities as well as some other utilities must adhere to this reporting requirement. The Electric Emergency Incident and Disturbance Report (Form OE-417) is used to collect and report relevant electric incidents and emergencies. See *Appendix C* for a copy of the form and submission instructions.

A representative from the utility legal team should advise the CIRT on all reporting requirements, participate in all reporting decisions, ensure reporting happens within required timelines, and review external messaging for legal and contractual compliance.

Develop Response Solutions and Assess Resource Needs

Once the incident is contained and a forensic investigation is complete, the CIRT should develop a plan to mitigate the incident, ensure the threat has been eradicated, and restore systems to normal operations. During this process, the utility should assess resource needs, including the type of expertise and the number of personnel required, hardware and software equipment needed, and replacement devices required, depending on the type of the incident. The Incident Response Manager should work with senior management to authorize the use of external response partners as necessary to determine and implement mitigation actions.

Enact Response Plan and Eradicate the Threat

Incident eradication should only be conducted after a complete investigation, and by an experienced team of cybersecurity experts. The CIRT should close any exposed vulnerabilities and remove the threat and any artifacts left by attackers (malicious code, data, etc.). This process should be rapid, thorough, and synchronized to avoid giving attackers time to cover their tracks or enact further damage. Eradication steps may include:

- Disabling breached user accounts and/or changing passwords
- Updating network intrusion detection system signatures to assess indicators of similar attacks in other parts of the environment
- Identifying exfiltrated data using packet capture (pcap) to assess network traffic
- Running a virus scanner to remove the compromised files or services
- Closing all network vectors of exfiltration and potential vectors for re-infection
- Informing employees of the threat or follow-up actions

Sophisticated or severe attacks may require the support of federal and industry experts to support investigation, mitigation planning, and eradication. *Section 3: Engaging Help* provides an overview of how to engage these resources during a significant event.

Incident Recovery and After-Action Review

Recover from an Incident

Succeeding incident eradication, utilities should restore the system to return to normal operation and detect and remedy vulnerabilities to prevent similar incidents. There are multiple ways to restore a system after an incident:

Remove the malicious artifacts and replace the compromised files with clean versions	Fast recovery time; cost-effective; might leave undiscovered artifacts behind
Restore from a back up	OK recovery time; cost-effective; only possible if known backup is unaffected
Rebuild the system(s) or environment	Slow recovery time; very costly; possibility of data loss; only way to rectify the affected processes if backups may be affected

The type of recovery is highly dependent on the nature of the incident and magnitude of damage to infrastructure. It is reasonable to assume that system backups may be affected, making it essential to check backups for viruses, rootkits, and other vulnerabilities before restoring from a backup.

If a backup is unavailable, the system must be reinstalled from scratch. After re-install (including the operating system), all known vulnerabilities should be remediated. This includes actions such as installing patches; changing passwords; changing accounts; and tightening the network security perimeter (e.g., changing firewall and boundary router access control lists). The newly remediated system should be validated for both security and business functions before it is put back online.

At the conclusion of the incident response, management should receive an after-action report on the incident, the response, lessons learned, and any follow-on activities or recommendations including changes to the incident response plans or participation in mutual assistance agreements.

Conduct After-Action Review

Following incident recovery, utilities should assess response activities to verify attack vectors are eradicated and ensure steps are taken to prevent similar attacks in the future. Potential post-incident actions include:

1. **Create and track recovery metrics**. Use data and specific metrics to measure effectiveness of system recovery. Potential metrics may include:
   a. Patch Policy Compliance
   b. Mean Time to Patch; Vulnerability Scan Coverage
   c. % of Systems without Known Severe Vulnerabilities
   d. Mean Time to Incident Discovery
   e. Incident Rate; % of Incidents Detected
2. **Strengthen network security**. Enhance system monitoring, administrative policies, and other protective measure to limit future risk of similar incidents and increase security.
3. **Document findings**. Record threat assessment, procedures, roles and responsibilities, metrics tracking, and process adjustments.
4. **Report mitigations**. If deemed appropriate, in consultation with legal counsel, report the incident and subsequent response actions to the ISACs for industry situational awareness.
5. **Refresh security training**. Schedule re-training on relevant security protocols, send "refresher" emails to key employers on security guidelines, and identify additional training to prevent similar incidents in the future.

5 STRATEGIC COMMUNICATION PROCEDURES

A Cyber Incident Response Plan should designate a POC within the Cyber Incident Response Team to manage and coordinate internal and external communications. This POC could be a member of the utility's external relations, public affairs, communications, or customer service departments. As with other incident response roles, the plan should also designate a back-up POC to ensure availability and provide extra coverage during the incident—especially in the early stages of response, during high-impact incidents, or during an incident with significant media interest.

To protect the privileged nature of communications, legal counsel should direct the incident investigation. Legal should also review and approve all external communications related to a cyber incident. While the communications team and POC will develop and coordinate external messaging among the CIRT, all documentation and messaging should be done only with the knowledge and at the direction of the legal counsel overseeing incident response.

Working with the utility's legal counsel, the communications team should develop Cyber Incident Communication Procedures that:

- Identify all potential stakeholder groups that may require communication, including internal stakeholders (e.g., managers/executives, municipal officials, employees, Board of Directors) and external stakeholders.
- Determine what type of information each stakeholder needs, and who on the CIRT can provide or verify the accuracy of that information. While internal communications may be more complete than external communications, all communication should be made on a need-to-know basis.
- Outline the expected timing of key messaging and any triggers of additional alerts or notifications.
- Identify the distinct communication methods and needs of stakeholders directly involved in incident response versus non-response stakeholders.

Response Stakeholders: Depending on the size of the incident and the response team, other CIRT members outside of the communications team might be designated to communicate directly with external groups that are actively working alongside or providing information to the technical response team. These groups could include law enforcement, cybersecurity and incident response service providers, industry associations (e.g., APPA, E-ISAC, MS- ISAC), and other utilities. The utility communications team may support messaging for several of these response resources, but direct communications are more likely between technical team members. See "Engage Expert Response Resources" in *Section 3: Engaging Help* for additional considerations on notifying and communicating with these stakeholders.

Non-Response Stakeholders: The following guidance primarily focuses on situational awareness communications with internal and external stakeholders who are not actively engaged in the technical response.

These may include:

- Employees—especially those whose job functions may be affected by the cyber incident
- Customers
- Media
- State/local leaders who must stay apprised of the incident

Communication Timing

During an active cyber incident investigation, the utility's timing for notifying employees, customers, business partners and the media will turn on applicable legal requirements and the status of the investigation and other response activities. Certain cyber incidents may merit early communications *during* incident response. Examples include:

- An incident that significantly impacts energy delivery or operations, particularly if extended or widespread outages are expected.
- An incident that affects access to customer-facing systems, such as billing and payment systems, online customer accounts/dashboards, or the company

website. The utility may want to notify customers about which systems are impacted and how long they expect the outage to be.

- An incident that has been widely reported in the media, such as an attack or vulnerability in common electricity industry devices or systems, especially if the utility has already been named or speculated as a target in media reports. In that event, expect media inquiries even if the incident has had limited or no impact on utility systems.
- An incident that affects some or all employees' ability to access key business systems, such as email, file servers, workstations, databases, or software applications. Only affected employees may need to be alerted, depending on the scope of affected systems.
- An incident that requires employees to take some action to help mitigate the incident, such as logging off of systems or reporting suspicious emails.

Media Reporting Considerations

The communications POC should coordinate all media messaging and act as or designate a spokesperson to interface with media representatives. This will ensure messaging is controlled and consistent. CIRT members and employees should be instructed to not discuss the incident outside the organization and direct all media inquiries to the designated POC.

During an incident that involves media engagement, it will be critical to have prepared and coordinated talking points, statements, or press releases to disseminate to media groups. Key messaging for these communications may include the following:

- Confirm the incident and communicate response plans and actions.
- Report involvement and cooperation with law enforcement or external response organizations. Do not speculate on the investigation and refer the media to the appropriate organization.
- Emphasize the utility's top priority is ensuring continued service or restoring service as soon as possible.
- Provide information or updates, as appropriate, on the incident impacts to power delivery or customer-facing systems.
- Commit to providing regular updates and identify where media or customers can find additional information.
- Manage expectations regarding cyber incidents and affirm that the utility is following its plans and procedures for cyber incident response.
- Thank customers for their patience.

Consider the following guidelines to facilitate more effective communications with media entities:

- **Identify local media contacts in advance** of an incident to build trust and familiarity.
- **Provide updates in a timely manner and when promised** to avoid speculation and misinformation, as reporters must meet tight deadlines
- **Keep information clear and concise**. Avoid jargon and highly technical explanations.
- **Coordinate messaging with the electricity industry**. A public power joint action agency or state association may have media expertise or talking points to leverage, and APPA's in-house public affairs team can help supplement or amplify media communications. APPA also works with the Electricity Subsector Coordinating Council (ESCC) on behalf of members to coordinate industry-wide messaging during incidents affecting the electricity industry.
- **Leverage mutual assistance for media communications**. The ESCC utilities leverage media staff from other utilities to manage media communications during a significant incident, including tracking and managing messaging through social media.

Once incident response and recovery have concluded, the utility may need to communicate that service has been restored, and emphasize the utility's commitment to review and enhance cybersecurity measures to prevent similar incidents in the future.

Customer and Employee Reporting Considerations

The utility should work with its legal team to identify the required process and timing for notifying affected individuals in the event that customer or employee personal data is compromised during a cyber incident. Data breaches should be disclosed to the media in consultation with the legal team and in accordance with applicable breach notification laws or requirements. The utility may be subject to federal, state, and/or municipal notification requirements.

In any incident, only convey information that is accurate and confirmed, and do not include speculation. Consider the following elements in messages to employees and/or customers:

- Short description of the incident (e.g., data breach, billing system outage) and date(s) the incident occurred.
- Type and nature of the personal data compromised, or the systems and functions impacted.
- Reassurance that measures are being taken by the utility to prevent a future incident/data breach.
- Steps that the customer/employee may need to take.
- Contact information for further information.

Communication Templates

The following templates for communicating information to public stakeholders were drawn from the Electricity Subsector Coordinating Council (ESCC) Playbook, Version 9.0, July 2018. The Playbook outlines a process for coordinated response among the energy industry during significant incidents, including cyber events.

The ESCC uses the Traffic Light Protocol (TLP) for informational use and dissemination. These sample questions and templates are marked TLP: GREEN. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. For more information, see: *www.us-cert.gov/tlp*.

Cyber Incident that Disrupts Power

Sample Template for Media Statement/Press Release

Confirm the incident and communicate response plans and actions.

- [UTILITY NAME] is responding to a cyber incident affecting our networks.
- Upon learning of this incident, [UTILITY NAME] activated our cyber incident response plan and launched an analysis and investigation to determine the nature and scope of the incident. We also notified our industry and government partners to coordinate on mitigating risk to other organizations.
  - *Additional language if the company is a member of the Cyber Mutual Assistance Program and would like to acknowledge that it has requested assistance:*

    In addition, [UTILITY NAME] has secured additional expertise/assistance to investigate and respond to this incident through the electric power industry's Cyber Mutual Assistance program. This program is based on the industry's traditional mutual assistance programs and is designed to help electric companies restore critical systems following cyber incidents.
  - *Additional language if the company would like to acknowledge that it is working with industry organizations:*

    [UTILITY NAME] has also notified and is working with relevant electricity industry organizations, including [the American Public Power Association, the Electricity Information Sharing and Analysis Center, the Multi-State Information Sharing and Analysis Center] to coordinate response.
- At this stage, our primary goal is to restore service to the customers who have been affected by this incident as quickly and safely as possible.
  - *If able to report*: As of [date/time], there are [number] of customers without power.
  - *If able to report*: Provide additional details on response crews and restoration priorities, similar to non-cyber events.
- We are also working to understand how the incident occurred and to identify ways to prevent similar incidents from occurring in the future.
- The investigation into the incident is ongoing. We are coordinating with local and federal authorities, including [the FBI, the Department of Homeland Security, and the Department of Energy]. Please contact [the FBI and/or local law enforcement authorities] for specific information regarding their activities.

Commit to providing regular updates and identify resources for additional information.

- We will continue to monitor the situation and provide updates to keep our customers informed of any developments.
- For the most current information, please visit [UTILITY WEBSITE] or call [NUMBER].
  - *Alternative language if company website is offline*: Due to the incident, our company website [and online transactions—including bill payments—] have been suspended temporarily. Customers should visit [URL] or call [NUMBER] for more information.
- *If applicable*: We will post updates to our social media channels, including [Facebook, Twitter, etc.]. You can find us on Facebook at [NAME] and on Twitter, @[HANDLE].
- *If known*: We expect to provide additional media briefings at [LOCATION] on [DATE/TIME].

Manage expectations regarding cyber incidents.

- We make it a top priority to understand the dynamic cyber threat environment, and we work closely with [other electric companies, and with government and cross-sector partners,] to protect our infrastructure from cyber breaches and the loss of sensitive information.
- We understand that no single solution exists that can eliminate risk completely. And, no company can guarantee that its cybersecurity systems and protection protocols will be successful 100 percent of the time. For these reasons, we also develop plans to respond and recover quickly when incidents impact our systems or infrastructure. We now are using those plans to respond to this ongoing incident.

Thank customers for their patience.

- We know that being without electricity creates hardships for our customers, and we appreciate their patience as our crews work around the clock to respond to this incident.
- Please know that we are doing what we can, when we can, and where we can to restore power safely and as quickly as possible.

Key Questions to Consider

Prepare to face the following questions from reporters, customers, and response officials:

- What has happened?
- Are additional attacks expected?
- Was power disrupted and for how long?
- How many customers were impacted?
- Was customer personal information compromised?
- Do we expect additional attacks or issues?
- Were other electric companies targeted?
- What steps is the company taking to respond and restore service?
- Has the government and law enforcement been notified? Are you coordinating with them in any way?
- Was this terrorism or a coordinated attack?
- Was this an act of war?
- Is there a sense of who the culprit is and how long they were inside the affected electric company's network / system? Was it days, weeks, or months?

- How long will it take to return to normal operations?
- What assets or operations have been affected?
- How long do you anticipate the issues to last?
- Has this happened before?
- Does the company conduct cyber attack exercises or drills?
- Did the company know there was a risk? If so, what did you do to try to mitigate against the attack? If not, what are you doing to prevent or better anticipate these types of cyber threats in the future?

Cyber Incident that Does Not Disrupt Power (e.g., data breach, disruption of customer-facing systems)

Sample Template for Media Statement/Press Release

Confirm the incident and communicate response plans and actions.

- [UTILITY NAME] is responding to a cyber incident affecting our networks.
- Upon learning of this incident, [UTILITY NAME] activated our cyber incident response plan, launched an assessment of the nature and scope of the incident, and notified appropriate industry and government partners.
- *If verified*: Those organizations are now alerting the electric power industry and other critical infrastructure sectors so they can prepare for, or can prevent, similar incidents.
  - *Additional language if the company is a member of the Cyber Mutual Assistance Program and would like to acknowledge that it has requested assistance:*

    In addition, [UTILITY NAME] has secured additional expertise/assistance to investigate and respond to this incident through the electric power industry's Cyber Mutual Assistance program. This program is based on the industry's traditional mutual assistance programs and is designed to help electric companies restore critical systems following cyber incidents.
  - *Additional language if the company would like to acknowledge that it is working with industry organizations:*

    [UTILITY NAME] has also notified and is working with relevant electricity industry organizations, including [the American Public Power Association, the Electricity Information Sharing and Analysis Center, the Multi-State Information Sharing and Analysis Center] to coordinate response.
- We are working to understand how the incident occurred, quickly return to normal operations, and to identify ways to prevent similar incidents from occurring in the future.
- The investigation into the incident is ongoing. We are coordinating with local and federal authorities, including [the FBI, the Department of Homeland Security, and the Department of Energy]. Please contact [the FBI and/or local law enforcement authorities] for specific information regarding their activities.

Commit to providing regular updates and identify resources for additional information.

- While the response is still under way, we can report that, at this time, no power disruptions have occurred as a result of the incident. We will continue to monitor the situation and provide updates to keep our customers informed of any developments.
- [Include information about any disruptions to customer-facing sites and any actions customers should take regarding bill payments or service requests.]

- For the most current information, please visit [UTILITY WEBSITE] or call [NUMBER].
  - *Alternative language if company website is offline*: Due to the incident, our company website [and online transactions—including bill payments—] have been suspended temporarily. Customers should visit [URL] or call [NUMBER] for more information.
- *If applicable*: We will post updates to our social media channels, including [Facebook, Twitter, etc.]. You can find us on Facebook at [NAME] and on Twitter, @[HANDLE].

Manage expectations regarding cyber incidents.

- No company can guarantee that its cybersecurity systems and protection protocols will be successful 100 percent of the time, which is why we have a cyber incident response plan in place and have fully activated that plan to respond effectively.
- We make it a top priority to understand the dynamic cyber threat environment and protect our infrastructure from cyber breaches and the loss of sensitive information. We understand that no single solution exists that can eliminate risk completely. We work closely with [other electric companies, and with government and cross-sector partners,] to manage these cyber risks.

Thank customers for their patience.

- We thank all of our customers for their patience as we respond to this cyber incident.
- Protecting our customers' information and delivering safe, reliable energy are our top priorities. We understand how this incident has impacted our customers, and we sincerely apologize for any inconvenience or concern this incident has caused.
- We are working around the clock to identify all issues and to restore our systems and services to normal operating order.

Key Questions to Consider

Prepare to face the following questions from reporters, customers, and response officials:

- What happened and when?
- What systems or sites are affected?
- What kind of information was compromised?
- Do you expect more information to be compromised?
- What protocols are in place to safeguard this information?
- Do you know how this happened and who the culprit is?
- Have other companies been targeted?
- How long were the culprits in the electric utility's network? Was it days, weeks, or months?
- How many customers were affected?
- Do customers and employees need to do anything to safeguard their information?
- When did the breach occur?
- Was the risk known? If so, what did you do to try to mitigate against the attack? If not, what are you doing to try and better anticipate these types of cyber threats in the future?
- Is there a history of this happening before?
- What are the next steps to resolving this issue?

6 CYBER INCIDENT RESPONSE LEGAL PROCEDURES

A utility's legal team, both internal and through outside counsel, must be central to its cyber incident response plan. Utilities should develop Cyber Incident Legal Response Procedures to guide the implementation of legal team responsibilities under such plans. These Procedures should apply to every cyber incident and should address legal requirements in the event of a cyber incident. To that end, utilities' cyber incident response processes, procedures, and plans should include requirements to promptly alert the legal team of a cyber incident. Upon becoming aware of a cyber incident, the legal team should consult its Cyber Incident Response Legal Procedures. The legal team should be responsible for implementing, interpreting, reviewing, and complying with the Procedures.

Preserving Legal Posture

In parallel with the early containment, remediation, and investigation efforts associated with a cyber incident, the legal team should take steps to help preserve a utility's legal posture by directing and approving relevant documentation and preservation efforts, including through:

- Maintaining a chain of custody for documents and other physical evidence, preserving relevant system logs, creating backups of affected files, and maintaining historical backups to show the affected system's prior state.
- Issuing legal hold notices applicable to the relevant records.
- Preserving privilege by retaining outside experts, directing the utility's investigation of the cyber incident, and directing any documentation of the cyber incident.
- Preparing non-disclosure and information sharing agreements with third parties in connection with the cyber incident.
- Seeking to limit the unauthorized disclosure or use of sensitive information that has been exposed in connection with the cyber incident.

Retaining Outside Experts

In consultation with the appropriate business unit, the legal team should be responsible for retaining outside counsel, outside technology or forensic experts, private investigators, outside public relations firms, or other third-party experts to assist in response to a cyber incident. The legal team should also be responsible for directing any third-party investigations, including the preparation of any documentation relating to a third-party investigation and determining if and how the findings may be documented.

Contacting Law Enforcement and Information Security Organizations

The legal team, in consultation with the incident response team, should direct reporting of a cyber incident to relevant law enforcement authorities. The legal team should also determine whether to cooperate in law enforcement efforts.

The incident response team should consult the legal team before notifying external information security and cybersecurity organizations. The legal team should assist the incident response team in determining whether there is a duty to make such a notification, and should review the content of the notification for compliance with legal requirements.

Reviewing Insurance Policies and Contacting Insurance Providers

The legal team should review a utility's applicable insurance policies to determine (1) how coverage amounts impact expenses incurred in connection with the cyber incident, and (2) any policy obligations to notify an insurance provider prior to incurring such expenses. As necessary, the appropriate business unit, at the direction of the legal team, should notify a utility's relevant insurer of the cyber incident. The legal team, in collaboration with the appropriate business unit, should pursue cyber insurance coverage to facilitate maximum recovery under a utility's relevant insurance policies.

Managing Public and Government Relations and Internal Communications

The legal team should work with Communications to develop an external communications plan and coordinate messaging to media and determine appropriate utility representatives to serve as spokespersons regarding the cyber incident.

The legal team should work with the appropriate business unit to develop an internal communications plan and coordinate messaging to the utility's leadership and other personnel.

The legal team should also work with the appropriate business unit to develop and implement a government relations plan (such as notifications to members of Congress), as appropriate.

Communications with Service Providers and Business Partners

A utility's service providers and business partners may be required to notify the utility of certain cyber incidents. When receiving such a notification, the legal team should inform the appropriate individuals identified in the utility's incident response plan. In consultation with the incident response team, the legal team should work with the service provider or business partner to:

- Investigate the reported cyber incident.
- Coordinate implementation of the utility's Cyber Incident Response Legal Procedures.
- Confirm that the service provider or business partner follows a process that complies with the Procedures and with all applicable legal requirements;

If the utility has a legal or contractual obligation to notify any of its service providers or business partners of a cyber incident, or otherwise chooses to do so, the legal team should investigate and coordinate all related activities.

Evaluating Notification and Reporting Obligations

The legal team should evaluate the circumstances of a cyber incident to determine whether any applicable laws, regulations, contracts, or industry requirements or standards require the utility to notify persons or entities of the cyber incident. The legal team may consider, among other factors:

- Whether the specific data elements or systems affected by the cyber incident trigger a notification requirement under applicable legal requirements.
- Whether the cyber incident triggers a reporting obligation to a government agency.
- Whether sensitive information may be in the physical possession or control of an unauthorized person or downloaded, copied, or used by an unauthorized person.
- Whether potentially affected individuals have reported unusual account activity.
- Whether the cyber incident poses a risk of fraud, identity theft or other harm to affected individuals.
- Whether the cyber incident triggers a disclosure obligation under financial reporting requirements.

The legal team should review the contract with the relevant service provider or business partner and seek legal remedy, indemnification, or reimbursement, as appropriate.

If a cyber incident is determined to trigger a notification or reporting requirement, the legal team should review any required communications for accuracy.

Identifying and Notifying Affected Individuals

If a cyber incident involves personal information, the legal team should conduct an investigation to identify affected individuals for notification purposes. The legal team should direct and document the investigation.

When a utility has identified the individuals or groups likely to have been affected by the cyber incident, it should notify them based on advice from the legal team,

in accordance with applicable law. The utility should provide notification to affected individuals in accordance with the timing, format, and content requirements of applicable laws. The notice to affected individuals should be clear and conspicuous, and written using easy-to-understand language.

If necessary, the legal team should enter into contracts with relevant third parties to assist in the notification process or provide related services (for example, credit monitoring or identity protection, call center, and mail house or email distribution services).

Notifying Consumer Reporting Agencies and Payment Card Entities

Where required by law or otherwise appropriate, the legal team should provide written notification of a cyber incident affecting personal information to the three U.S. nationwide consumer reporting agencies (Equifax, Experian, and TransUnion).

If information relating to payment cards is reasonably believed to have been acquired or accessed by an unauthorized person during a cyber incident, the legal team should notify the relevant payment card brands and processing entities in accordance with the utility's contractual obligations, and should comply with applicable payment card brand requirements.

Notifying Regulatory Agencies

As required by law or as advisable, the legal team, in coordination with the appropriate business unit, should provide timely written notification of the cyber incident to relevant regulatory authorities.

Regulatory Follow-Up, Litigation, and Post-Incident Remediation

In the aftermath of a cyber incident, the legal team, in coordination with appropriate business units, should:

- Respond to inquiries or enforcement actions by regulatory authorities in connection with a cyber incident.
- Lead any related litigation activities, whether such activities are proactive (such as bringing an action against a culpable service provider) or reactive (including responding to a lawsuit); and take appropriate remedial actions to address the cyber incident, such as recommending disciplinary actions or invoking contractual obligations included in any agreement with the party responsible for the cyber incident.

7 SAMPLE CYBER INCIDENT SCENARIOS

The following cyber incident scenarios provide an example of all five categories of incidents and how the incident response procedures might be followed at a typical public power utility. The scenarios are not designed to prescribe response steps to an individual utility. Rather, utilities can use them to begin outlining response procedures for each category of incident and examine gaps in the incident response plan.

Level 1 Incident

Threat

A utility's IT analyst discovers an unregistered IP address on the network.

Potential utility actions under the scenario threat include the following:

Incident Assessment

- IT immediately notifies the Cyber Incident Response Manager.
- Cyber Incident Response Manager assigns IT support to investigate the unregistered IP address.

Incident Eradication & Recovery

- IT support is unable to identify indicators of compromise and isolates the unregistered IP address to an on-site contractor.
- Contractor's IP address is registered on the network after a full review of their network activities.

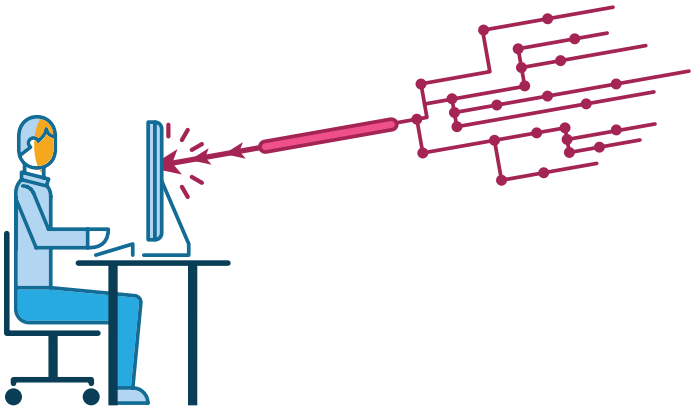
Post-Incident Response

- Cyber Incident Response Manager sends email to utility management staff stressing the importance of contacting IT prior to providing network access to contractors.

Level 2 Incident

Threat

Phishing attack targets utility senior management and creates a persistent threat by installing zero-day malware that exploits vulnerabilities in their Windows systems, collecting network credentials and harvesting unclassified proprietary information. IT detects abnormal levels of network traffic.



Potential utility actions under the scenario threat include the following:

Incident Assessment

- IT immediately notifies the Cyber Incident Response Manager.
- The Cyber Incident Response Manager assigns a severity level to the incident and informs the CIRT Steering Committee. The Steering Committee confirms the severity level and mobilizes the CIRT to conduct an investigation at the direction of counsel, identify indicators of compromise, and identify which critical assets, if any, may be affected.
- After measuring the characteristics of vital business and operational processes and referring to older logs, the CIRT confirms that the IT network has been breached.

- The incident response manager notifies senior management and business continuity groups. A mitigation strategy is developed.
- Counsel and the finance department determine the business and legal impact of information breach.
- The CIRT conducts a full forensic investigation at the direction of counsel to determine the full magnitude and depth of the attack.

Incident Containment

- The CIRT contains and isolates the breach by disconnecting affected devices from the internet.
- The CIRT contacts third party security support staff for additional monitoring and response support.

Incident Reporting

- The CIRT notifies state/local law enforcement to file a criminal complaint against suspected actors responsible for cyber incident.

Incident Eradication & Recovery

- The CIRT removes all components associated with the incident, runs a virus/malware scanner to remove compromised files, updates signatures, and disables executive's user account.
- The CIRT restores system to normal operation by cleaning the malicious artifacts and replacing compromised files.

Post-Incident Response

- In coordination with legal counsel, the Cyber Incident Response Manager disseminates an after-action report to utility staff.
- The CIRT enhances system monitoring, administrative policies, and other protective measure to limit future risk of similar incidents and increase security.
- If deemed appropriate, the CIRT reports mitigation measures to the MS-ISAC and E-ISAC.

Level 3 Incident

Threat

The utility's cybersecurity monitoring service alerts the utility's cybersecurity manager of unusual network activity. After an initial assessment, the utility's cybersecurity team determines that their network has been exposed to malware that is potentially exfiltrating customer social security numbers and credit card information.

Potential utility actions under the scenario threat include the following:

Incident Assessment

- The cybersecurity manager notifies the Cyber Incident Response Manager (if it is a separate individual) of the incident.
- Cyber Incident Response Manager assigns a severity level to the incident and informs the CIRT Steering Committee. The Steering Committee confirms the severity level and mobilizes the CIRT—including management, IT and OT personnel, communications/ public affairs, business continuity group, business lines—to conduct an investigation at the direction of counsel and with the assistance of a third-party forensic investigator, identify which critical assets or systems are affected, and determine the extent and nature of the compromise.
- The CIRT confirms that business enterprise network is compromised, and sensitive customer information is being exfiltrated.

Incident Containment

- The CIRT and third-party vendor grasp that this

incident is beyond the utility's internal capabilities and engages the third-party forensic investigator through legal counsel to assist with containment and response support.

Incident Reporting

- Utility voluntarily reports the incident to the MS-ISAC, which confirms the malware has been used to target other state agency networks that contain sensitive personal information. The utility also reports the incident to the E-ISAC and APPA for industry situational awareness.
- The CIRT notifies federal/state/local law enforcement to seek assistance and file a criminal complaint against suspected actors responsible for cyber incident.

Incident Eradication & Recovery

- The utility coordinates with the MS-ISAC and APPA, who interface with DHS NCCIC to supply the utility with recommended mitigation actions specific to the malware.
- The utility's CIRT develops a mitigation and communication strategy.
- The CIRT, with the assistance of the forensic investigator, completes the investigation, safely takes affected systems offline, assesses the operational impact, and determines if backup systems are compromised. The CIRT considers sending data or other information from the incident to the MS-ISAC for additional analysis.
- The team applies patches, updates anti-virus signature files, runs virus clean up, restores the affected system from back-up, and takes other steps to eradicate the malware and recover from the incident.

Post-Incident Response

- Utility notifies affected individuals of the data breach in accordance with applicable legal requirements.
- The utility prepares a holding statement in the event of media inquiries.
- The CIRT Steering Committee oversees after an action review of the utility's response to the incident, and identifies areas for improvement.
- The CIRT enhances system monitoring, administrative policies, and other protective measures to limit future risk of similar incidents and increase security.
- If deemed appropriate, the CIRT reports mitigation measures to the MS-ISAC and E-ISAC.

Level 4 Incident

Threat

The utility's cybersecurity team receives an alert indicating that a specific vendor's intelligent electronic device, which is used in the utility's substations, has been compromised. The device is susceptible to malware designed to access firmware in industrial control and SCADA systems.

Potential utility actions under the scenario threat include the following:

Incident Assessment

- Cybersecurity team notifies the Cyber Incident Response Manager of the alert.
- The Cyber Incident Response Manager assigns the incident a severity level and notifies the CIRT Steering Committee, which confirms the severity level and convenes the CIRT—including management, IT and OT personnel, legal, and HR. The CIRT assesses the threat to identify indicators of compromise and which critical assets, if any, may be affected by the vulnerability.
- The CIRT contacts the vendor's technical support to identify potential mitigations. The vendor informs the utility it is working on a patch and identifies steps the utility can take to determine whether the vulnerable devices have been potentially compromised.

- The CIRT continues to work with vendor and E-ISAC to ensure that other vendor products are free of vulnerabilities.

Incident Containment

- Crews are dispatched to affected substations to monitor for unusual activity, inspect equipment condition, and pull logs.
- The intelligent electronic device is temporarily taken offline. Temporary manual controls are put in place while the utility's cybersecurity team investigates whether the vulnerable devices were actually compromised.

Incident Reporting

- Cyber Incident Response Manager/federal compliance representative reports the incident to NERC and/or DOE, if required.
- Cyber Incident Response Manager reports the threat to other utilities in the Cyber Mutual Assistance (CMA) Program and consults with them to validate initial containment and response actions. The Cyber Incident Response Manager alerts APPA of a potential incident, alerting them that additional resources may be needed if the assessment reveals that operational systems were compromised.

Incident Eradication & Recovery

- Further assessment shows that there is no evidence of malware and no indication that the vulnerable devices were compromised.
- The vendor releases a patch for the vulnerability, which requires all affected devices to be updated and tested. The utility makes a request through the CMA Program for additional technical support in patching and verifying devices quickly.

Post-Incident Response

- The CIRT Steering Committee oversees an after-action review of the utility's response to the incident, and identifies areas for improvement. The CIRT enhances system monitoring, administrative policies, and other protective measures to limit future risk of similar incidents and increase security.
- If deemed appropriate, the CIRT reports mitigation measures to the MS-ISAC and E-ISAC.

Level 5 Incident

Threat

Attackers utilize spear phishing tactics to obtain access credentials to a utility's business and industrial control system (ICS) networks. These actors simultaneously used HMIs in the SCADA environment to target substation field devices and upload malicious firmware to ethernet gateway devices, ensuring remote commands could not be issued to bring substations back online. Numerous substations were out of service for up to 3 hours, affecting hundreds or thousands of customers.

Potential utility actions under the scenario threat include the following:

Incident Assessment

- Operations staff notifies Cyber Incident Response Manager of operational issues that may indicate a cyber attack.
- The Cyber Incident Response Manager assigns the incident a severity level and notifies the CIRT Steering Committee, which confirms the severity level and convenes the CIRT—including management, IT and OT personnel, legal, public affairs, HR, compliance, business continuity, and key business lines. The CIRT begins to determine which critical assets may be affected, conduct triage, and assess manual workarounds for all key processes to ensure business continuity.

Incident Reporting

- The Cyber Incident Response Manager and/or federal compliance representative, in coordination with legal counsel, reports the incident to NERC if CIP assets are affected.
- The CIRT notifies the local FBI Field Office, which is coordinating with other FBI Field Offices to investigate similar reports from other utilities. The CIRT also notifies state/local law enforcement to file a criminal complaint against suspected actors responsible for the cyber incident.
- The utility reports the incident to the E-ISAC, which confirms that several other utilities have reported similar incidents over the last 24 hours. The utility contacts APPA, which has begun coordinating with the ESCC and federal incident response officials at DHS and DOE.

Incident Containment

- Utility takes compromised equipment offline and shifts to manual processes for monitoring and control where possible.
- Response will require highly technical cyber resources and expertise beyond what the utility or vendors can provide.

Incident Eradication & Recovery

- APPA activates the ESCC Crisis State Activity and immediately begins engaging with federal response groups (e.g., DHS, DOE) and developing unified messaging across stakeholder groups.
- DHS and DOE deploy teams to several affected utilities, in coordination with FBI Field Offices, to investigate the attack and determine mitigations.
- The utility works with onsite teams and third-party vendors to investigate the nature and extent of the attack, at the direction of legal counsel, remove affected equipment, assess backups for malware, and clean affected systems without further impacting power delivery.
- Utility replaces compromised devices and works with the third-party vendor to ensure new devices are configured securely and adequately tested.
- APPA and the ESCC work with the media to provide coordinated messages as affected utilities respond to the incident and recover. The utility releases messages via press releases and social media providing accurate information on the attack and the number of customers affected, and sharing recovery and response actions, as appropriate. Messages are updated as appropriate when new information becomes available.
- The utility continues to work with the FBI to provide access to systems, networks, and logs, as appropriate, to inform incident investigation.

Post-Incident Response

- The CIRT Steering Committee oversees an after-action review of the utility's response to the incident and identifies areas for improvement. The CIRT enhances system monitoring, administrative policies, and other protective measure to limit future risk of similar incidents and increase security.
- If deemed appropriate, the CIRT reports mitigation measures to the MS-ISAC and E-ISAC.

Appendix A: Incident Response Plan Outline

I. Introduction

A. **Overview**: Explain that the utility is committed to safeguarding operational and information technology, but that the risk of a Cyber Incident remains. The Incident Response Plan is to assist the utility in promptly identifying, evaluating, responding to, investigating, and resolving Cyber Incidents impacting utility systems.

B. **Scope**: The Incident Response Plan should apply to every Cyber Incident. Provide contact information for individuals in utility's information security team and legal team for further questions about the Incident Response Plan.

C. **Delegation**: Employees should have the ability to delegate Incident Response Plan roles and responsibilities assigned to them to employees under their direct supervision, provided that final responsibility rests with the delegating employee.

D. **Incident Response Plan Summary**: Provide a brief summary of the Incident Response Plan's structure and general responsibilities.

E. **Confidentiality and Privilege**: Statement on the need for communications to remain confidential. To maintain privilege, the legal team should lead all aspects of the investigation of a Cyber Incident.

F. **Definitions**: Define terms necessary for the Incident Response Plan, such as the following:

- *Confidential Business Information*: All information maintained, owned, or controlled by a utility, or on behalf of a utility by a third party, that is not publicly known or whose access is restricted internally by the utility.
- *Cybersecurity Event*: Any observable occurrence suggesting possible actual or attempted unauthorized access to a utility's systems.
- *Cyber Incident*: Reasonably suspected (1) loss or exposure of Protected Information, or (2) actual or attempted unauthorized access to a utility's systems that threatens the confidentiality, integrity, or availability of those systems through (A) the acquisition, use, disclosure, modification, or destruction of Protected Information or (B) interference with a process, a function, or data on the utility's or a third-party's information system that adversely impacts the utility's business operations.
- *Cyber Incident Response Team ("CIRT")*: Utility personnel and external support providers designated by the CIRT Steering Committee who are responsible for developing and implementing an overall strategy for responding to a Level 2 (Moderate) or Level 3 (High) Cyber Incident, or as otherwise appropriate.
- *CIRT Steering Committee*: Utility personnel responsible for managing and implementing the Incident Response Plan, including assembling and overseeing the CIRT. The CIRT Steering Committee should be limited in size and include members of the information security team and legal team.
- *Personal Information*: Any individually identifiable information from or about an individual, including customers, employees, or any other individual.
- *Protected Information*: All information, including Confidential Business Information and Personal Information, that is maintained, owned, or controlled by a utility, or on behalf of a utility by a third party, that is not publicly known or whose access is restricted internally by the utility.

II. Incident Identification and Classification

A. **Detection**: Describe the means by which a utility may discover evidence of a Cybersecurity Event.

B. **Reporting**: Provide a phone number and/or e-mail for employees to contact when becoming aware of a Cybersecurity Event.

C. **Triage**: List initial response and triage activities by information security team when notified of a cybersecurity event, including reporting to a supervisor.

D. **Classification**: Cyber Incidents should be classified by one of five severity levels. The information security team can declare a Level 1 (Low) Cyber Incident. Cyber Incidents suspected of being in the range from a Level 2 (Medium) to a Level 5 (High) Cyber Incident should be reported to the head of the information security team, who should notify the CIRT Steering Committee.

III. Incident Escalation

A. **Level 5 (High) Cyber Incident**: Describe escalation process for Level 5 incidents, e.g., CIRT Steering Committee convenes the CIRT, senior executives are notified, and outside counsel is retained.

B. **Level 4 Cyber Incident**: Describe escalation process for Level 4 incidents.

C. **Level 3 Cyber Incident**: Describe escalation process for Level 3 incidents.

D. **Level 2 Cyber Incident**: Describe escalation process for Level 2 incidents.

E. **Level 1 (Low) Cyber Incident**: Describe escalation process for Level 1 incidents, e.g., First Response Team is solely responsible for responding to incident, but can consult with Legal as appropriate.

IV. Incident Response

A. **CIRT**: The CIRT Steering Committee should determine the number of members and composition of the CIRT. The CIRT should develop and implement an overall strategy for responding to the Cyber Incident, which involves a determination of how best to coordinate the response. The CIRT Steering Committee should assign an Incident Response Manager to lead the CIRT.

B. **Investigation, Containment and Remediation**: Legal should oversee the investigation of the incident in conjunction with the Incident Response Manager. The head of the information security team should determine whether to engage outside forensic experts, who should be retained by the legal team. The head of the information security team, in coordination with the CIRT, should determine what actions should be taken to contain, control and remediate the Cyber Incident. To the maximum extent feasible, while containing and remediating the Cyber Incident, affected systems should not be shut down or altered in any manner without prior approval from legal team. If it is not feasible to seek the legal team's approval of such actions in advance, then the legal team should be promptly notified.

C. **Notifications**: The legal team should determine whether any applicable laws, contracts, or industry requirements or standards require the Company to notify government agencies or officials, third party entities, or affected persons of a Cyber Incident. The legal team should be responsible for all notifications required pursuant to a legal obligation to government agencies or officials, third party entities, or individuals affected by a Cyber Incident.

D. **Contacting Law Enforcement**: In coordination with the CIRT, the legal team should direct the reporting of a Cyber Incident to relevant law enforcement authorities.

E. **Voluntary Information Sharing**: The information security team may engage in anonymous voluntary threat information sharing at any time, but should consult the legal team before voluntarily sharing non-anonymous information regarding a Cyber Incident.

F. **Managing External Communications**: A utility's external communications team should develop and implement an external communications plan in consultation with the legal team and CIRT.

G. **Managing Employee Communications**: A utility's human resources team should develop and implement an employee communications plan in consultation with the legal team and CIRT.

H. **Managing Government Affairs**: A utility's government affairs team should develop and implement a government relations plan in consultation with the legal team and CIRT.

V. Post-Incident Remediation

A. **Regulatory Follow-Up and Litigation**: The legal team in coordination with a utility's government affairs team should respond to any regulatory inquiries or enforcement actions. The legal team should lead any litigation-related activities.

B. **Post-Mortem Analysis**: The head of a utility's information security team should conduct a root cause analysis of a Cyber Incident and report findings to the CIRT Steering Committee. As appropriate, the CIRT Steering Committee should conduct a "lessons learned" meeting concerning an incident with relevant stakeholders, and document any lessons learned or document the absence of lessons learned.

VI. Incident Response Plan Maintenance

Describe how the CIRT Steering Committee will organize, test, and update the Incident Response Plan, as appropriate.

VII. Appendices

Include essential response resources as appendices, such as:

A. **Cyber Incident Severity Classification Chart**: Chart identifying the standard for classifying Cyber Incidents at each of the five severity levels, including relevant factors to consider when making that classification.

B. **Incident Response Plan Roles and Responsibilities**: A list of employee and entity roles and responsibilities under the Incident Response Plan.

C. **Incident Plan Internal Contact List**: An internal contact list of utility employees, and their alternates, who could be called upon to act under the Incident Response Plan.

D. **External Support providers**: Contact information for external support providers, such as outside counsel, forensic experts, and direct mail companies (for notifications), who could be called upon to act under the Incident Response Plan.

Appendix B: Incident Handling Form Templates

Incident handling guides shown below were modeled after SANS Institute *templates*. Incident handling forms are intended for internal use. The utility's legal team should oversee incident investigation, and all incident documentation should be done at the direction of legal counsel.

CYBER INCIDENT RESPONSE HANDLING FORMS **PAGE ___ OF ___**

CYBER INCIDENT CONTACT LIST **DATE UPDATED: _____**

Cyber Incident Response Team

Cyber Incident Response Manager

Name: .....

Title: .....

Phone: .....

Mobile: .....

E-mail: .....

Address: .....

.....

Chief Counsel

Name: .....

Title: .....

Phone: .....

Mobile: .....

E-mail: .....

Address: .....

.....

IT Technical Lead

Name: .....

Title: .....

Phone: .....

Mobile: .....

E-mail: .....

Address: .....

.....

OT Technical Lead

Name: .....

Title: .....

Phone: .....

Mobile: .....

E-mail: .....

Address: .....

.....

Public Affairs Lead

Name: .....

Title: .....

Phone: .....

Mobile: .....

E-mail: .....

Address: .....

.....

Legal Affairs Personnel

Name: .....

Title: .....

Phone: .....

Mobile: .....

E-mail: .....

Address: .....

.....

SAMPLE CRITICAL ASSET INVENTORY LIST **DATE UPDATED: _____**

The North American Electric Reliability Corporation (NERC) report *Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets* was referenced in developing the sample critical asset inventory list below.

Power Generator	[Entity-specific identifier]	123.123.1.2	**Turbine Control System**	**[HIGH] [MEDIUM] [LOW]**
Power Generator	[Entity-specific identifier]	123.123.1.2	**Integrated Plant Control**	
Power Generator	[Entity-specific identifier]	123.123.1.2	**Continuous Emissions Monitoring System (CEMS)**	

Control Center	[Entity-specific identifier]	123.123.1.2	**SCADA Supervisory Control**	**[HIGH] [MEDIUM] [LOW]**
Control Center	[Entity-specific identifier]	123.123.1.2	**State Estimator**	
Control Center	[Entity-specific identifier]	123.123.1.2	**Print Server**	

Transmission Substation	[Entity-specific identifier]	123.123.1.2	**Protective Relaying**	**[HIGH] [MEDIUM] [LOW]**
Transmission Substation	[Entity-specific identifier]	123.123.1.2	**Phasor Measurement Unit (PMU)**	
Transmission Substation	[Entity-specific identifier]	123.123.1.2	**Special Protection Systems (SPS)**	

Incident Detector Information

Name: .....

Title: .....

Phone: .....

Mobile: .....

E-mail: .....

Organization: .....

.....

Date and Time Detected: .....

.....

Initial Response Action: .....

.....

Additional Information: .....

.....

.....

Incident Summary

Type of Incident Detected:

☐ Denial of service (DoS) ☐ Malware ☐ SQL injection ☐ Cyber-physical

☐ Phishing ☐ Man-in-the-middle attack ☐ Zero-day exploit

Incident Information:

Attack Vector: .....

Function: .....

Asset: .....

Site (if applicable): .....

Point of Contact: .....

Phone: .....

Mobile: .....

Email: .....

Address: .....

How was the Incident Detected: .....

.....

.....

.....

.....

Additional Information: .....

.....

.....

.....

.....

.....

INCIDENT CONTAINMENT **DATE UPDATED:** _____

Isolate impacted systems:

Cyber Incident Response Team Manager approved removal from network? ☐ YES ☐ NO

If YES, date and time systems were removed: .....

If NO, state the reason: .....

.....

.....

Backup impacted systems:

System backup successful for all systems? ☐ YES ☐ NO

Name of persons who performed backup: .....

.....

.....

.....

.....

Backup start date and time: .....

Backup completion date and time: .....

Backup tapes sealed? ☐ YES ☐ NO Seal Date: .....

Backup tapes contact: .....

Backup location: .....

Name: ..... Date: .....

Signature: .....

INCIDENT ERADICATION DATE UPDATED: _____

Name of persons and organizations performing forensics on systems:

Name: ..... **Organization:** .....
Phone: ..... Email: .....

Name: ..... **Organization:** .....
Phone: ..... Email: .....

Name: ..... **Organization:** .....
Phone: ..... Email: .....

Was the vulnerability and attack vector identified? ☐ YES ☐ NO
Describe: .....

.....

.....

.....

.....

.....

.....

.....

.....

What was the validation procedure used to ensure the incident was fully eradicated?
Describe: .....

.....

.....

.....

.....

.....

.....

.....

.....

Appendix C: DOE Electric Emergency Incident Disturbance Report (OE-417)

DOE, under its relevant authorities, has established mandatory reporting requirements for electric emergency incidents and disturbances in the United States. The Electric Emergency Incident and Disturbance Report (Form OE-417) collects information on electric incidents and emergencies. Schedule 1 and lines 13-17 in Schedule 2 of the form must be submitted to the DOE only when at least one of the twelve criteria on page one of the form is met. The Form OE-417 must be filed either within one hour or six hours of the incident. Requirements specific to cyber events are bolded below:

Physical attack that causes major interruptions	Physical attack that could potentially impact electric power system adequacy or reliability
Cyber event that causes operation interruptions	**Cyber event that could potentially impact power adequacy or reliability**
Operational shutdown or shut-down of the transmission and/or distribution electrical system	Loss of service to more than 50,000 customers for 1 hour or more
Electrical System Separation (Islanding)	Fuel supply emergencies that could impact power system adequacy or reliability
Uncontrolled loss of 300 MW or more for more than 15 minutes	
Load shedding of 100 MW or more	
System-wide voltage reductions of 3% of more	
Public appeal to reduce use of electricity to maintain power continuity	

Electric utilities that operate as reliability coordinators or balancing authorities as well as other utilities—in cases where a balancing authority or reliability coordinator is not involved—must adhere to this reporting requirement. Failure to do may result in criminal fines, civil penalties, and other sanctions as permitted by law.

DOE Report Filing

Submit DOE-OE-417 Event Reporting Form via one of the following:

- Online: *www.oe.netl.doe.gov/OE417/*
- Fax: (202) 586-8485
- Telephone: (202) 586-8100

DOE's OE-417 reporting form shown below can be found on DOE's National Energy Technology Laboratory (NETL) *website*.

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	*ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT*	OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

NOTICE: This report is **mandatory** under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. **Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.**

RESPONSE DUE:

Within 1 hour of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as an Emergency Alert report if criteria 1-8 are met.
Within 6 hours of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as a Normal Report if only criteria 9-12 are met.
By the later of 24 hours after the recognition of the incident OR by the end of the next business day submit Schedule 1 & lines M - Q in Schedule 2 as a System Report if criteria 13-24 are met. *Note: 4:00pm local time will be considered the end of the business day*

Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident.
For NERC reporting entities registered in the United States; NERC has approved that the form OE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.

METHODS OF FILING RESPONSE
(Retain a completed copy of this form for your files.)

Online:	Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/
FAX:	FAX Form OE-417 to the following facsimile number: (202) 586-8485.
Alternate:	If you are unable to submit online or by fax, forms may be e-mailed to doehqeoc@hq.doe.gov, or call and report the information to the following telephone number: (202) 586-8100.

SCHEDULE 1 -- ALERT CRITERIA

(Page 1 of 4)

Criteria for Filing (Check all that apply)
See Instructions For More Information

EMERGENCY ALERT **File within 1-Hour** If any box 1-8 on the right is checked, this form must be filed within 1 hour of the incident; check Emergency Alert (for the Alert Status) on **Line A** below.	1. [ ] Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations 2. [ ] Cyber event that causes interruptions of electrical system operations 3. [ ] Complete operational failure or shut-down of the transmission and/or distribution electrical system 4. [ ] Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system 5. [ ] Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single incident 6. [ ] Firm load shedding of 100 Megawatts or more implemented under emergency operational policy 7. [ ] System-wide voltage reductions of 3 percent or more 8. [ ] Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System
NORMAL REPORT **File within 6-Hours** If any box 9-12 on the right is checked AND none of the boxes 1-8 are checked, this form must be filed within 6 hours of the incident; check Normal Report (for the Alert Status) on **Line A** below.	9. [ ] Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems 10. [ ] Cyber event that could potentially impact electric power system adequacy or reliability 11. [ ] Loss of electric service to more than 50,000 customers for 1 hour or more 12. [ ] Fuel supply emergencies that could impact electric power system adequacy or reliability

SCHEDULE 1 -- ALERT CRITERIA -- CONTINUED

(Page 2 of 4)

SYSTEM REPORT
File within 1-Business Day

If any box 13-24 on the right is checked AND none of the boxes 1-12 are checked, this form must be filed by the later of 24 hours after the recognition of the incident OR by the end of the next business day. *Note:* 4:00pm local time will be considered the end of the business day. Check System Report (for the Alert Status) on **Line A** below.

13. [ ] Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in action(s) to avoid a Bulk Electric System Emergency.

14. [ ] Damage or destruction of its Facility that results from actual or suspected intentional human action.

15. [ ] Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.

16. [ ] Physical threat to its Bulk Electric System control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. Or suspicious device or activity at its Bulk Electric System control center.

17. [ ] Bulk Electric System Emergency resulting in voltage deviation on a Facility; A voltage deviation equal to or greater than 10% of nominal voltage sustained for greater than or equal to 15 continuous minutes.

18. [ ] Uncontrolled loss of 200 Megawatts or more of firm system loads for 15 minutes or more from a single incident for entities with previous year's peak demand less than or equal to 3,000 Megawatts

19. [ ] Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.

20. [ ] Complete loss of off-site power (LOOP) affecting a nuclear generating station per the Nuclear Plant Interface Requirements.

21. [ ] Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).

22. [ ] Unplanned evacuation from its Bulk Electric System control center facility for 30 continuous minutes or more.

23. [ ] Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability affecting its staffed Bulk Electric System control center for 30 continuous minutes or more.

24. [ ] Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.

If significant changes have occurred after filing the initial report, re-file the form with the changes and check Update (for the Alert Status) on **Line A** below.

The form must be re-filed within 72 hours of the incident with the latest information and Final (Alert Status) checked on **Line A** below, unless updated

LINE NO.						
A.	Alert Status (check one)	Emergency Alert [ ] 1 Hour	Normal Report [ ] 6 Hours	System Report [ ] 1 Business Day	Update [ ] As required	Final [ ] 72 Hours
B.	Organization Name					
C.	Address of Principal Business Office					

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	*ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT*	OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

SCHEDULE 1 -- ALERT NOTICE

(Page 3 of 4)

INCIDENT AND DISTURBANCE DATA

D.	Geographic Area(s) Affected (County, State)			
E.	Date/Time Incident Began (mm-dd-yy/hh:mm) using 24-hour clock	____ - ____ - ____ / ____ : ____ mo dd yy hh mm	[ ] Eastern [ ] Central [ ] Mountain [ ] Pacific [ ] Alaska [ ] Hawaii	
F.	Date/Time Incident Ended (mm-dd-yy/ hh:mm) using 24-hour clock	____ - ____ - ____ / ____ : ____ mo dd yy hh mm	[ ] Eastern [ ] Central [ ] Mountain [ ] Pacific [ ] Alaska [ ] Hawaii	
G.	Did the incident/disturbance originate in your system/area? (check one)	Yes [ ]	No [ ]	Unknown [ ]
H.	Estimate of Amount of Demand Involved (Peak Megawatts)		Zero [ ]	Unknown [ ]
I.	Estimate of Number of Customers Affected		Zero [ ]	Unknown [ ]

SCHEDULE 1 – TYPE OF EMERGENCY

Check all that apply

J. Cause	K. Impact	L. Action Taken
☐ Unknown ☐ Physical attack ☐ Threat of physical attack ☐ Vandalism ☐ Theft ☐ Suspicious activity ☐ Cyber event (information technology) ☐ Cyber event (operational technology) ☐ Fuel supply emergencies, interruption, or deficiency ☐ Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure ☐ Transmission equipment failure (not including substation or switchyard) ☐ Failure at high voltage substation or switchyard ☐ Weather or natural disaster ☐ Operator action(s) ☐ Other ☐ Additional Information/Comments:	☐ None ☐ Control center loss, failure, or evacuation ☐ Loss or degradation of control center monitoring or communication systems ☐ Damage or destruction of a facility ☐ Electrical system separation (islanding) ☐ Complete operational failure or shutdown of the transmission and/or distribution system ☐ Major transmission system interruption (three or more BES elements) ☐ Major distribution system interruption ☐ Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more ☐ Loss of electric service to more than 50,000 customers for 1 hour or more ☐ System-wide voltage reductions or 3 percent or more ☐ Voltage deviation on an individual facility of ≥10% for 15 minutes or more ☐ Inadequate electric resources to serve load ☐ Generating capacity loss of 1,400 MW or more ☐ Generating capacity loss of 2,000 MW or more ☐ Complete loss of off-site power to a nuclear generating station ☐ Other ☐ Additional Information/Comments:	☐ None ☐ Shed Firm Load: Load shedding of 100 MW or more implemented under emergency operational policy (manually or automatically via UFLS or remedial action scheme) ☐ Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system ☐ Implemented a warning, alert, or contingency plan ☐ Voltage reduction ☐ Shed Interruptible Load ☐ Repaired or restored ☐ Mitigation implemented ☐ Other ☐ Additional Information/Comments

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	*ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT*	OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours

SCHEDULE 2 -- NARRATIVE DESCRIPTION

Information on Schedule 2 will not be disclosed to the public to the extent that it satisfies the criteria for exemption under the Freedom of Information Act, e.g., exemptions for confidential commercial information and trade secrets, certain information that could endanger the physical safety of an individual, or information designated as Critical Energy Infrastructure Information.

NAME OF OFFICIAL THAT SHOULD BE CONTACTED FOR FOLLOW-UP OR ANY ADDITIONAL INFORMATION		
M.	Name	
N.	Title	
O.	Telephone Number	( )-( )-( )
P.	FAX Number	( )-( )-( )
Q.	E-mail Address	

Provide a description of the incident and actions taken to resolve it. Include as appropriate, the cause of the incident/disturbance, change in frequency, mitigation actions taken, equipment damaged, critical infrastructures interrupted, effects on other systems, and preliminary results from any investigations. Be sure to identify: the estimate restoration date, the name of any lost high voltage substations or switchyards, whether there was any electrical system separation (and if there were, what the islanding boundaries were), and the name of the generators and voltage lines that were lost (shown by capacity type and voltage size grouping). If necessary, copy and attach additional sheets. Equivalent documents, containing this information can be supplied to meet the requirement; this includes the NERC EOP-004 Disturbance Report. **Along with the filing of Schedule 2, a final (updated) Schedule 1 needs to be filed. Check the Final box on line A for Alert Status on Schedule 1 and submit this and the completed Schedule 2 no later than 72 hours after detection that a criterion was met.**

R. Narrative:

S. Estimated Restoration Date for all Affected Customers Who Can Receive Power	____ - ____ - ____ mo dd yy
T. Name of Assets Impacted	

U. Notify NERC/E-ISAC	Select if you approve of all of the information provided on the Form being submitted to the North America Electric Reliability Corporation (NERC) and/or the Electricity Information Sharing and Analysis Center (E-ISAC) NERC is an entity that is certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk power system but that is not part of the Federal Government. This information would be submitted to help fulfill the respondent's requirements under NERC's reliability standards. If approval is given to alert NERC and/or E-ISAC the Form will be emailed to systemawareness@nerc.net and/or operations@eisac.com when it is submitted to DOE. DOE is not responsible for ensuring the receipt of these emails by NERC and/or E-ISAC. ☐ Notify NERC | ☐ Notify E-ISAC

Appendix D: Sample Cyber Mutual Assistance Program NDA

The following non-disclosure agreement (NDA) is used by all participating members of the Electricity Subsector Coordinating Council's (ESCC) Cyber Mutual Assistance (CMA) program. The sample NDA below was updated as of June 2016. For updated information and the most reecent NDA, visit *www.electricitysubsector.org/CMA/*. See "Cyber Mutual Assistance Process" in *Section 3: Engaging Help* for more information on how mutual assistance works.

Mutual Non-Disclosure and Use of Information Agreement to Support Emergency Cyber Mutual Assistance

This Non-Disclosure and Use of Information Agreement (the "Agreement'') is made and entered into as of this 15th day of June, 2016 by and among each entity that executes and delivers the signature page to this Agreement (each, a "Participating Entity" and collectively, the "Participating Entities").

A. Each Participating Entity is participating in a voluntary effort to assist the Electricity Subsector Coordinating Council (ESCC) in developing and implementing one or more industry initiatives to provide cyber emergency assistance to entities in the electric sector (collectively, the "Cyber Mutual Assistance Program").

B. In connection with the Cyber Mutual Assistance Program, each Participating Entity may voluntarily choose to request from or provide to another Participating Entity emergency cyber mutual assistance in response to a cyber emergency;

C. The development and implementation of any Cyber Mutual Assistance Program, including any request or provision of cyber mutual assistance between Participating Entities, may necessitate the exchange of certain confidential or proprietary information.

NOW, THEREFORE, in consideration of the mutual covenants in this Agreement, the Participating Entities agree as follows:

1. Purpose, Scope, and Definitions. The purpose of this Agreement is to permit each Participating Entity to exchange Confidential Information (as defined below) as needed to pursue the development and implementation of a Cyber Mutual Assistance Program, including any request for or provision of cyber mutual assistance between Participating Entities in response to a cyber emergency or in connection with any Cyber Mutual Assistance Program.

"Confidential Information" under this Agreement consists of:

i. all information disclosed by any Participating Entity, or any of its employees, directors, officers, affiliates, partners, agents, advisors or other representatives ("Representatives") pursuant to that Participating Entity's participation in or contribution to the development or implementation of a Cyber Mutual Assistance Program, including any Participating Entity's request for or provision of cyber mutual assistance, whether disclosed prior to or following the execution of this Agreement;

ii. any information or documentation produced by a Participating Entity, or any of its Representatives, under any Cyber Mutual Assistance Program or related to a specific request for or response to cyber mutual assistance, including any analysis of such information, and whether produced prior to or following the execution of this Agreement;

iii. any aggregation, consolidation, or listing of information or documentation disclosed by one or more Participating Entities, or any of their respective Representatives, pursuant to the development or implementation of a Cyber Mutual Assistance Program including any Participating Entity's request for or provision of cyber mutual assistance; and

iv. all observations of equipment (including computer screens) and oral disclosures related to the development of any Cyber Mutual Assistance Program or a specific request for or response to cyber mutual assistance, including the systems, operations, and activities of each Participating Entity, whether such observations or oral disclosures were made prior to or following the execution of this Agreement.

2. Non-Disclosure and Use of Confidential Information. Each Participating Entity agrees (i) to maintain the confidentiality of all Confidential Information obtained, (ii) without the express permission of the Participating Entity providing such information, not to disclose such information to third parties, and (iii) to use such information only for the express purpose of developing and implementing a Cyber Mutual Assistance Program, including in connection with any request for or provision of cyber mutual assistance between Participating Entities. Each Participating Entity shall use the Confidential Information received hereunder only for the purposes identified in Section 1. Notwithstanding the forgoing, a Participating Entity may use and internally share Confidential Information as deemed necessary to respond to an actual or threatened cyber emergency that places, or has the potential to place, the Participating Entity's cyber systems at risk. Any other use shall be only with the prior written consent of the Participating Entity or Participating Entities that provided the Confidential Information sought to be used.

3. Exemptions to Non-Disclosure. Notwithstanding Sections 1 and 2, a Participating Entity shall not have breached any obligation under this Agreement if the Confidential Information is disclosed to a third party when the Confidential Information:

A. was in the public domain at the time of such disclosure or is subsequently made available to the public by the Participating Entity who provided the Confidential Information, or otherwise consistent with the terms of this Agreement; or

B. had been received or independently developed by such Participating Entity at or prior to the time of disclosure through a process other than the development or implementation of the Cyber Mutual Assistance Program; or

C. is subsequently disclosed to the Participating Entity by a third party without restriction on use and without breach of any agreement or legal duty; or

D. subject to the provisions of Section 4, is used or disclosed pursuant to statutory duty, such as a public records act request, or an order, subpoena, discovery request, or other lawful process issued by a court or other governmental authority of competent jurisdiction or in a judicial proceeding; or

E. is disclosed by unanimous agreement of each of the Participating Entity or Participating Entities whose information is subject to such disclosure; or

F. after the time of its disclosure hereunder, becomes subsequently available to such Participating Entity on a non-confidential basis from a source not known by such Participating Entity to be bound by a confidentiality agreement or secrecy obligation in respect thereof.

4. Notice of Pending Third-Party Disclosure or Unauthorized Disclosure.

A. In the event that any governmental authority issues an order, subpoena, or other lawful process or a Participating Entity receives a discovery request in a civil proceeding ("Legal Process") requiring the disclosure of any Confidential Information, the Participating Entity receiving such Legal Process shall notify in writing the other Participating Entities within five (5) business days of receipt. The Participating Entity receiving such Legal Process shall not be in violation of this Agreement if it complies with the Legal Process requiring disclosure of the Confidential Information after seven (7) business days following Participating Entity notification, as set forth above.

B. A Participating Entity shall not disclose any Confidential Information in response to a request under the federal Freedom of Information Act, 5 U.S.C. § 552, as amended, or an equivalent state or local open records law, except as required by law as determined in the written opinion of such Participating Entity's legal counsel. Upon receipt of a Freedom of Information Act or public records disclosure request, such Participating Entity shall: (i) notify each Participating Entity or Participating Entities whose information is subject to such disclosure request immediately upon receipt of a request for public records that include all or part of the Confidential Information; and (ii) if, in the written opinion of the legal counsel for the Participating Entity receiving the information request, the Confidential Information is not legally required to be disclosed, treat the requested Confidential Information as exempt from disclosure to the extent permitted by applicable law. The Participating Entity receiving the information request shall cooperate with the Participating Entity or Participating Entities whose information is subject to such disclosure request in challenging the request or seeking another appropriate remedy, as necessary. If such challenge to the request is not successful and another remedy is not obtained, only that portion of the Confidential Information that is legally required to be disclosed, as determined in the written opinion of the Participating Entity's legal counsel, shall be disclosed.

C. Unauthorized Disclosure: If a Participating Entity becomes aware that Confidential Information has been or likely has been disclosed to a third party in violation of this Agreement, the Participating Entity will immediately notify the Participating Entity in writing that provided the disclosed Confidential Information, provide a description of the information disclosed, and provide reasonable assistance to the Participating Entity that provided the disclosed Confidential Information to recover the Confidential Information and prevent further unauthorized disclosure.

5. Term. This Agreement shall remain in effect as to each Participating Entity unless and until a Participating Entity seeking to withdraw from the agreement provides ten (10) days' prior written notice to the other Participating Entities, then this Agreement shall terminate with respect to such Participating Entity at the conclusion of such ten (10) day period; provided, however, that termination shall not extinguish any claim, liability, or cause of action under this Agreement existing at the time of termination. The provisions of Sections 1, 2, 3, 4, 5 and 6 shall survive the termination of this Agreement for a period of ten (10) years.

6. Return or Destruction of Confidential Information. Upon termination of this Agreement, all Confidential Information in the possession or control of a Participating Entity and its Representatives that received such information shall be returned to the Participating Entity that disclosed the information, including all copies of such information in any form whatsoever, unless otherwise instructed in writing by the Participating Entity that disclosed the information. Notwithstanding the foregoing, if the Confidential Information is retained in the computer backup system of a Participating Entity, the Confidential Information will be destroyed in accordance with the regular ongoing records retention process of the Participating Entity. In lieu of return, a Participating Entity may certify to the other Participating Entities in writing that all such Confidential Information, in any form whatsoever, has been destroyed. Notwithstanding anything in this paragraph 6 to the contrary, a Participating Entity may retain a record copy of any Confidential Information if required to do so by applicable law. In such an instance, such Participating Entity shall identify in writing the specific Confidential Information retained, and shall provide the affected Participating Entity or Participating Entities with a written commitment to return or destroy the retained Confidential Information upon the expiration of the retention period required by law. The obligation under this Agreement to maintain the confidentiality of all Confidential Information shall continue to apply to such retained Confidential Information for so long as the Participating Entity possesses such Confidential Information.

7. Notices. All notices, requests, demands, and other communications required or permitted under this Agreement shall be in writing, unless otherwise agreed by the Participating Entities, and shall be delivered in person or sent by certified mail, postage prepaid, by overnight delivery, or by electronic mail or electronic facsimile transmission with an original sent immediately thereafter by postage prepaid mail, and properly addressed with respect to a particular Participating Entity, to such Participating Entity's representative as set forth on such Participating Entity's signature page to this Agreement. A Participating Entity may from time to time change its representative or address for the purpose of notices to that Participating Entity by a similar notice specifying a new representative or address, but no such change shall be deemed to have been given until such notice is actually received by the Participating Entity being so notified.

8. Complete Agreement; No Other Rights. This Agreement contains the complete and exclusive agreement of the Participating Entities with respect to the subject matter thereof. No change to this Agreement shall be effective unless agreed to in writing by all of the then existing Participating Entities. This Agreement is not intended to create any right in or obligation of any Participating Entity or third party other than those expressly stated herein.

9. No Warranties or Representations. Any Confidential Information disclosed under this Agreement carries no warranty or representation of any kind, either express or implied. A Participating Entity receiving such Confidential Information shall not be entitled to rely on the accuracy, completeness, or quality of the Confidential Information, even for the purpose stated in Section 1.

10. Injunctive Relief. Each Participating Entity agrees that, in addition to whatever other remedies may be available to the other Participating Entities under applicable law, the other Participating Entities shall be entitled to seek injunctive relief with respect to any actual or threatened violation of this Agreement by a Participating Entity or any third party receiving Confidential Information.

11. Choice of Law and Forum. This Agreement shall be governed by and construed in accordance with the laws of the State of New York without giving effect to any choice or conflicts of law provision or rule that would cause the application of laws of any other jurisdiction.

12. Assignment. This Agreement shall be binding upon the Participating Entities, their successors, and assigns. No Participating Entity may assign this Agreement without the prior written consent of the other Participating Entities.

13. Construction of Agreement. Ambiguities or uncertainties in the wording of this Agreement shall not be construed for or against any Participating Entity, but shall be construed in the manner that most accurately reflects the Participating Entities' intent as of the date they executed this Agreement.

14. Signature Authority. Each person signing below warrants that he or she has been duly authorized by the Participating Entity for whom he or she signs to execute this Agreement on behalf of that Participating Entity.

15. Counterparts. This Agreement may be executed in counterparts, all of which shall be considered one and the same Agreement.

IN WITNESS WHEREOF, the Participating Entities have executed this Agreement as of the date set forth above.

Dated: _____

Participating Entity:

By
Name: _____
Title: _____

Appendix E: Resources and References

Additional Planning Resources

The following resources may be of value to utilities as they develop or augment their cyber incident response plans and procedures.

National Institute of Standards and Technology (NIST):

1. *Computer Security Incident Handling Guide*, SP 800-61 Rev. 2, 2012
2. *Guide for Cybersecurity Event Recovery*, SP 800-184, 2016

SANS Institute:

1. *Sample Incident Handling Forms*
2. *Checklists & Step-by-Step Guides*
3. *Law Enforcement FAQ*, 2004

American Public Power Association (APPA):

1. *Cybersecurity Scorecard*
2. *Cybersecurity Roadmap*, 2019

Electricity Subsector Coordinating Council (ESCC):

1. *ESCC Playbook: A Crises Management Framework for the ESCC* (Available to ESCC members. Contact *secretariat@electricitysubsector.org* or visit *www.electricitysubsector.org* to learn more.)
2. *Cyber Mutual Assistance Program*

U.S. Department of Homeland Security (DHS):

1. *US CERT Federal Incident Notification Guidelines*, 2017
2. *National Cyber Incident Response Plan*, 2016